#4

LAW OFFICES OF

JACOBSON HOLMAN

PROFESSIONAL LIMITED LIABILITY COMPANY

400 SEVENTH STREET, N. W.

WASHINGTON, D. C. 20004

(202) 638-6666

HARVEY B. JACOBSON, JR.
JOHN CLARKE HOLMAN
SIMOR L. MOSKOWITZ
ALLEN S. MELSER
MICHAEL R. SLOBASKY
MARSHA G. GENTNER
JONATHAN L. SCHERER
IRWIN M. AISENBERG
GEORGE W. LEWIS
WILLIAM E. PLAYER
YOON S. HAM
PHILIP L. O'NEILL
LINDA J. SHAPIRO
LEESA N. WEISS
SUZIN C. BAILEY*
MATTHEW J. CUCCIAS
DANIEL K. DORSEY
SUZANNAH K. SUNDBY*

YOON S. HAM
Direct: (202)662-8483
yham@jhip.com

JACOBSON HOLMAN STERN

OF COUNSEL
MARVIN R. STERN
NATHANIEL A. HUMPHRIES

TELEFAX:
(202) 393-5350
(202) 393-5351
(202) 393-5352

E-MAIL: IP@JHIP.COM
INTERNET: WWW.JHIP.COM

*BAR OTHER THAN DC

December 28, 2001

Atty. Docket No.: **P67500US0**
CUSTOMER NUMBER: 00136

Honorable Commissioner for Patents
Washington, D.C. 20231

Sir:

Transmitted herewith for filing is the patent application in the names of:

You Sung KANG of **Taejon, Republic of Korea**;
Sin Hyo KIM of **Taejon, Republic of Korea**;
Dae Hun NYANG of **Taejon, Republic of Korea**; and
Byung Ho CHUNG of **Taejon, Republic of Korea**,

for **METHOD OF SETTING COMMUNICATION ENVIRONMENT BETWEEN SMART CARD AND MOBILE TERMINAL USING LAYERED ARCHITECTURE OF PROTOCOL STACK**. The application comprises a 17-page specification including 7 claims (2 independents) and Abstract, 3 sheets of drawings (Figs. 1-3), and a Declaration and Power of Attorney.

Accompanying this application for filing are:

(1) Small Entity Declaration;
(2) Assignment document, cover sheet and **$40.00** fee for recordation of Assignment;
(3) A preliminary amendment to lessen fee;
(4) Information Disclosure Statement, PTO-1449 Form and Copies of References; and
(5) A certified copy of **Korean** Application No. **2001-76825**, filed **December 16, 2001**, the priority of which is claimed under 35 U.S.C. §119.

The filing fee has been calculated as shown:

Small Entity		$ 370.00
Total Claims=07;	in excess of 20 = 0 x ($09.00) =	0.00
Total Ind. Claims=02;	in excess of 03 = 0 x ($42.00) =	+ 0.00
	TOTAL FILING FEE:	**$ 370.00**

A check in the amount of **$410.00**, is enclosed to cover the total Filing Fee and an Assignment Recordation Fee. The Commissioner is hereby authorized to charge payment of any fees set forth in Sections 1.16 or 1.17 during the pendency of this application, or credit any overpayment, to deposit Account No. 06-1358. A duplicate copy of this sheet is enclosed.

Respectfully submitted,

By: _____
Yoon S. Ham, Reg. No. 45,307

Enclosures
YSH:ecl

대 한 민 국 특 허 청

KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 특허출원 2001년 제 76825 호
Application Number PATENT-2001-0076825

출 원 년 월 일 : 2001년 12월 06일
Date of Application DEC 06, 2001

출 원 인 : 한국전자통신연구원
Applicant(s) KOREA ELECTRONICS & TELECOMMUNICATIONS RESEARCH INST

2001 년 12 월 17 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【제출일자】	2001.12.06
【발명의 명칭】	계층화 구조의 프로토콜 스택을 사용하는 스마트 카드와 휴대 단말기의 통신 환경 설정 방법
【발명의 영문명칭】	Method for seting communication environment of smart card and mobile entity using layered protocol stack with selective multiple transmission protocols
【출원인】	
【명칭】	한국전자통신연구원
【출원인코드】	3-1998-007763-8
【대리인】	
【성명】	권태복
【대리인코드】	9-2001-000347-1
【포괄위임등록번호】	2001-057650-1
【대리인】	
【성명】	이화익
【대리인코드】	9-1998-000417-9
【포괄위임등록번호】	1999-021997-1
【발명자】	
【성명의 국문표기】	강유성
【성명의 영문표기】	KANG,You-Sung
【주민등록번호】	711102-1552823
【우편번호】	302-728
【주소】	대전광역시 서구 내동 서우아파트 103동 403호
【국적】	KR
【발명자】	
【성명의 국문표기】	김신효
【성명의 영문표기】	KIM,Sin-Hyo
【주민등록번호】	680221-2645910
【우편번호】	305-390

【주소】 대전광역시 유성구 전민동 462-4 나래아파트 102동 703호

【국적】 KR

【발명자】

【성명의 국문표기】 양대헌

【성명의 영문표기】 NYANG,Dae-Hun

【주민등록번호】 701028-1140816

【우편번호】 405-234

【주소】 인천광역시 남동구 간석4동 579-1 23/2

【국적】 KR

【발명자】

【성명의 국문표기】 정병호

【성명의 영문표기】 CHUNG,Byung-Ho

【주민등록번호】 640208-1558710

【우편번호】 302-754

【주소】 대전광역시 서구 월평3동 진달래아파트 110동 105호

【국적】 KR

【심사청구】 청구

【취지】 특허법 제42조의 규정에 의하여 위와 같이 출원합니다. 대리인
권태복 (인) 대리인
이화익 (인)

【수수료】

【기본출원료】	20	면	29,000 원
【가산출원료】	3	면	3,000 원
【우선권주장료】	0	건	0 원
【심사청구료】	7	항	333,000 원

【합계】 365,000 원

【감면사유】 정부출연연구기관

【감면후 수수료】 182,500 원

【첨부서류】 1. 요약서·명세서(도면)_1통

【요약서】

【요약】

계층화 구조의 프로토콜 스택을 사용하는 스마트 카드와 휴대 단말기의 통신 환경 설정 방법은, 휴대 단말기와 스마트 카드 각각의 내부에 다수의 애플리케이션과 다수의 통신 환경을 보유하며, 전송 데이터의 송수신을 담당하는 전송 계층과 상기 송수신 데이터의 처리를 담당하는 응용 계층이 구분되어 구현되어 있으며, 상기의 스마트 카드가 응답하는 리셋 후 응답은 지원 가능한 통신 환경에 대한 정보를 모두 포함하고 있기 때문에, 스마트 카드와 휴대 단말기 사이의 통신 환경을 설정하고자 하는 경우에 해당 애플리케이션에 가장 적합한 통신 환경을 동적으로 구축할 수 있는 것이다. 따라서, 스마트 카드를 사용하는 휴대 단말기 사용자에게 신속하고 안정적인 통신 채널을 제공할 수 있는 것이다. 특히 본 발명에 따른 계층화 구조의 프로토콜 스택을 사용하는 스마트 카드와 휴대 단말기에서는 해당 애플리케이션에 대해 가장 적합한 통신 환경을 제공하기 때문에, 스마트 카드가 지니는 중요 정보의 저장과 처리 기능을 사용하고자 하는 이동 통신 시스템의 다양한 애플리케이션에 적용되어 이동 통신에서의 스마트 카드 활성화에 기여할 수 있는 효과가 있다.

【대표도】

도 2

【색인어】

스마트카드, 전송계층, 응용계층, 프로토콜, 파라미터, 논리채널

【명세서】

【발명의 명칭】

계층화 구조의 프로토콜 스택을 사용하는 스마트 카드와 휴대 단말기의 통신 환경 설정 방법{Method for seting communication environment of smart card and mobile entity using layered protocol stack with selective multiple transmission protocols}

【도면의 간단한 설명】

도 1은 종래의 스마트 카드 시스템에서 통신 속도와 통신 프로토콜 및 해당 어플리케이션을 결정하는 동작 흐름도.

도 2는 본 발명에 따른 계층화 구조의 프로토콜 스택을 사용하는 스마트 카드와 휴대 단말기 사이에서 통신 속도와 통신 프로토콜 및 해당 어플리케이션을 결정하는 동작 구성도,

도 3은 본 발명에 따른 스마트 카드와 휴대 단말기의 일 실시 예에 따른 최적의 통신 환경 설정 방법에 대한 처리 동작을 설명하기 위한 흐름도.

<도면의 주요 부분에 대한 부호의 설명>

100: 스마트 카드

200: 휴대 단말기

110: 스마트 카드에서의 응용 계층

120: 스마트 카드에서의 전송 계층

210: 휴대 단말기에서의 응용 계층

220: 휴대 단말기에서의 응용 계층

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<11> 본 발명은 계층화 구조의 프로토콜 스택을 사용하는 스마트 카드와 휴대 단말기의 통신 환경 설정 방법에 관한 것으로서, 특히 휴대 단말기 사용자가 다양한 어플리케이션(Application)을 가진 멀티 어플리케이션 스마트 카드(Multi-application smart card)를 이용하고자 할 때, 보다 신속하고 안정적으로 각 어플리케이션에 적합한 최적의 데이터 전송 속도를 보장하기 위하여 계층화 구조의 프로토콜 스택을 사용하는 계층화 구조의 프로토콜 스택을 사용하는 스마트 카드와 휴대 단말기의 통신 환경 설정 방법에 관한 것이다.

<12> 일반적으로, 이동성이 보장되는 소형의 휴대 단말기에 사용되는 스마트 카드는 중요 정보의 저장과 처리를 담당한다.

<13> 종래의 스마트 카드는 하드웨어적인 제약(예를 들면, 프로세서 성능, 메모리 크기 등)으로 인하여 본연의 기능인 정보의 저장과 처리 측면에서 그 한계를 가지며, 이러한 하드웨어적 한계는 스마트 카드와 휴대 단말기 사이의 데이터 통신 속도와 통신 프로토콜의 선택에도 지대한 영향을 미친다.

<14> 또한 종래의 스마트 카드는 이러한 하드웨어적 한계로 인하여 단일 어플리케이션을 위한 사용형태를 지니고 있다.

<15> 이하, 종래 기술에 따른 스마트 카드 시스템에서의 통신 속도 및 통신 프로토콜 선택 절차에 대하여 첨부한 도면을 참조하여 살펴보기로 하자.

<16> 도 1은 종래의 스마트 카드 시스템에서의 통신 속도와 통신 프로토콜 선택 절차를 나타내는 동작 구성도이다.

<17> 도 1에 도시된 바와 같이, 스마트 카드(100)가 휴대 단말기(200)에 삽입되면 스마트 카드(100)에 전원이 인가되고(S101), 스마트 카드(100)는 가장 먼저 리셋 후 응답(ATR: Answer To Reset)을 휴대 단말기(200)에 응답한다(S102).

<18> 일반적으로, 상기 스마트 카드(100)에서 휴대 단말기(200)로 제공하는 리셋 후 응답 정보에는 스마트 카드(100)와 휴대 단말기(200) 사이에서 운용될 수 있는 통신 속도, 통신 프로토콜, 전압, 전류, 데이터 보호구간 등의 정보를 포함할 수 있다.

<19> 상기 리셋 후 응답 정보를 수신한 휴대 단말기(200)는 프로토콜/파라미터 선택(PPS: Protocol and Parameters Selection) 요청 메시지를 스마트 카드(100)로 전송하여(S103) 스마트 카드(100)와 휴대 단말기(200) 사이의 새로운 통신 환경을 구축하고자 시도할 수 있다.

<20> 만일 스마트 카드(100)가 휴대 단말기(200)의 프로토콜/파라미터 선택 메시지의 요청에 따라 새로운 통신 환경을 구축할 수 있다면, 스마트 카드(100)는 프로토콜/파라미터 선택 요청 메시지에 대한 응답 신호를 휴대 단말기(200)로 전송

하고(S104), 그렇지 않고 스마트 카드(100)가 휴대 단말기(200)의 프로토콜/파라미터 선택 요청을 지원할 수 없다면, 스마트 카드(100)는 새로운 리셋을 기다린다.

<21> 만일 휴대 단말기(200)에서 요청한 프로토콜/파라미터를 스마트 카드(100)가 지원할 수 있어 해당 프로토콜/파라미터를 선택 지원한 경우, 선택된 프로토콜과 파라미터를 가진 통신 환경으로 휴대 단말기(200)는 논리 채널을 열기 위한 명령을 스마트 카드(100)로 전송하고, 즉, 휴대 단말기(200)는 스마트 카드(100)로 논리 채널 열기 요청 메시지를 전송한다(S105).

<22> 따라서, 스마트 카드(100)는 상기 휴대 단말기(200)의 논리 채널 열기 요청에 대한 응답 메시지를 휴대 단말기(200)로 전송하는 것이다(S106).

<23> 이와 같은 과정을 통해 스마트 카드(100)와 휴대 단말기(200)가 성공적으로 논리 채널이 형성되었다면, 휴대 단말기(200)는 스마트 카드(100)로 어플리케이션 선택 요청 메시지를 전송한다(S107).

<24> 이에 스마트 카드(100)는 휴대 단말기(200)의 요청에 따라 어플리케이션을 선택하고, 어플리케이션 선택 응답 메시지를 휴대 단말기(200)로 전송함으로써, 어플리케이션 선택을 위한 초기 동작이 완료되는 것이다.

<25> 상기에서는 종래의 스마트 카드 시스템에서의 통신 속도와 통신 프로토콜 선택 절차와 해당 어플리케이션 선택에 대한 일반적인 동작을 기술하고 있지만, 실제적인 사용 형태에서는 하나의 스마트 카드는 하나의 어플리케이션을 위한 전

용 스마트 카드로 주로 사용되기 때문에 프로토콜/파라미터 선택 절차를 생략하여 구현되기도 한다.

<26> 또한 전용 스마트 카드와 해당 어플리케이션은 상호간의 전용 어플리케이션만을 고려하기 때문에 전송을 위한 프로그램과 어플리케이션 구동을 위한 프로그램 구현이 계층적 구현이 아니라 통합된 형태로 구현되는 경향이 많다.

<27> 이러한 구현 형태는 정해진 통신 속도와 통신 프로토콜 외에 다른 고속의 통신 환경을 지원할 수 없으며, 또한 상기의 구현 방법으로는 멀티 어플리케이션 카드로의 발전을 지원할 수 없는 단점이 있다.

【발명이 이루고자 하는 기술적 과제】

<28> 따라서, 본 발명은 상기한 종래 기술에 따른 문제점을 해결하기 위하여 안출한 것으로, 본 발명의 주된 목적은 멀티 어플리케이션 스마트 카드 시스템에 있어서, 각 어플리케이션에 대해 최적의 통신 환경을 신속하고 안정적으로 구축하기 위한 스마트 카드와 휴대 단말기를 제공함에 있다.

<29> 본 발명의 다른 목적은, 멀티 어플리케이션 스마트 카드 시스템에 있어 각 어플리케이션과 가장 적합한 통신 속도와 통신 프로토콜을 선택적으로 사용할 수 있도록 내부적으로 응용계층과 전송계층이 명확하게 계층화 구조로 구현된 스마트 카드와 휴대 단말기를 제공하는 것이다.

<30> 또한 본 발명의 또 다른 목적은, 멀티 어플리케이션 스마트 카드 시스템에 있어 스마트 카드 내부의 어플리케이션 정보와 각 어플리케이션을 지원할 수 있

는 통신 속도, 통신 프로토콜 등의 정보를 리셋 후 응답 메시지에 담아 보냄으로써 스마트 카드와 휴대 단말기 사이의 최적의 통신 환경을 구축하는 방법을 제공하는데 있다.

【발명의 구성 및 작용】

<31> 상기 목적을 달성하기 위하여 본 발명은, 스마트 카드와 휴대 단말기 각각의 내부에서 계층화 구조의 프로토콜 스택을 구성하고 있으며, 스마트 카드와 휴대 단말기 각각의 전송 계층은 스위칭이 가능한 다수의 통신 프로토콜을 갖는 구성상의 특징과 스마트 카드의 리셋 후 응답이 스마트 카드의 지원 가능한 통신 환경에 대한 정보를 전송하고, 휴대 단말기는 상기의 리셋 후 응답을 수신하여 이를 분석하여 휴대 단말기의 어플리케이션이 원하는 최적의 통신 환경을 구축하는 기능을 보유하는 것을 특징으로 한다.

<32> 본 발명에 따른 계층화 구조의 프로토콜 스택을 사용하는 스마트 카드와 휴대 단말기의 통신 환경 설정 방법의 일 측면에 따르면, 상기 휴대 단말기에서 스마트 카드에 전원을 인가하면, 스마트 카드는 인가되는 전원에 따라 리셋 후 응답 정보를 휴대 단말기로 전송하는 단계; 상기 스마트 카드로부터 전송되는 응답 정보가 휴대 단말기 자신이 요구한 응답 형식인 경우, 휴대 단말기는 스마트 카드에서 제공되는 응답 정보를 분석하여 현재 사용하고자 하는 어플리케이션에 가장 적합한 최적의 통신 환경을 설정하는 단계; 최적의 통신 환경이 설정되면, 휴대 단말기는 스마트 카드로 어플리케이션에 사용할 논리 채널을 열기 위한 요청 메시지를 전송하는 단계; 스마트 카드는 휴대 단말기로부터 수신한 논리 채널 열기

요청 메시지에 따라 논리 채널을 열고 그에 상응하는 응답 신호를 휴대 단말기로 전송하는 단계; 휴대 단말기는 어플리케이션에서 사용할 논리 채널을 열어 스마트 카드와 휴대 단말기 사이의 통신 채널을 확보하는 단계를 포함할 수 있다. 여기서, 상기 스마트 카드로부터 제공되는 응답 정보는, 운용 전압, 전류, 데이터 보호구간 정보, 스마트 카드 자신이 지원하는 통신 속도, 통신 프로토콜에 대한 상세한 정보 중 적어도 하나의 정보를 포함한다.

<33> 상기 스마트 카드에서 제공되는 응답 형식이 휴대 단말기에서 요구하는 응답 형식이 아닌 경우, 휴대 단말기에서는 프로토콜/파라미터 선택 절차를 수행할 것인지를 판단하는 단계; 상기 판단 결과, 휴대 단말기가 프로토콜/파라미터 선택 절차를 수행하고자 하는 경우에는 스마트 카드로 프로토콜/파라미터 선택 요청 메시지를 전송하는 단계; 상기 휴대 단말기로부터 프로토콜/파라미터 선택 요청 메시지를 수신한 스마트 카드는 스마트 카드 내부에서 프로토콜/파라미터 선택 절차를 지원하는지를 판단하는 단계; 판단 결과, 스마트 카드 내부에서 프로토콜/파라미터 선택을 지원하는 경우 프로토콜/파라미터 선택 응답 메시지를 휴대 단말기로 전송하여 스마트 카드와 휴대 단말기간의 통신 채널을 확보하는 단계를 포함한다.

<34> 상기 스마트 카드 내부에서 프로토콜/파라미터 선택 절차를 지원하는지를 판단하는 단계에서, 스마트 카드 내부에서 프로토콜/파라미터 선택 절차를 지원하지 않는 경우에는 휴대 단말기로부터 리셋 신호가 오기를 기다리는 리셋 대기 상태로 전환하는 단계를 포함한다.

<35> 상기 스마트 카드와 휴대 단말기는, 전송 데이터의 송수신을 담당하는 전송 계층과 상기의 송수신 데이터를 처리하는 응용 계층을 각각 구비한다.

<36> 상기 스마트 카드와 휴대 단말기의 상기 응용 계층은, 다수의 어플리케이션을 구비하고, 상기 전송 계층은 상기 응용 계층의 다수의 어플리케이션을 지원할 수 있는 다수의 통신 환경을 보유하고 있다.

<37> 상기 전송 계층과 응용 계층이 상호 독립적으로 구현되어 하나의 어플리케션이 다수의 통신 프로토콜을 지원 받고, 하나의 통신 프로토콜이 다수의 어플리케이션을 지원할 수 있는 것이다.

<38> 한편, 본 발명에 따른 계층화 구조의 프로토콜 스택을 사용하는 스마트 카드와 휴대 단말기의 통신 환경 설정 방법을 수행하기 위하여 디지털 처리장치에 의해 실행될 수 있는 명령어들의 프로그램이 유형적으로 구현되어 있으며, 디지털 처리장치에 의해 판독될 수 있는 기록 매체의 일 측면에 따르면, 상기 휴대 단말기에서 스마트 카드에 전원을 인가하면, 스마트 카드는 인가되는 전원에 따라 리셋 후 응답 정보를 휴대 단말기로 전송하는 단계; 상기 스마트 카드로부터 전송되는 응답 정보가 휴대 단말기 자신이 요구한 응답 형식인 경우, 휴대 단말기는 스마트 카드에서 제공되는 응답 정보를 분석하여 현재 사용하고자 하는 어플리케이션에 가장 적합한 최적의 통신 환경을 설정하는 단계; 최적의 통신 환경이 설정되면, 휴대 단말기는 스마트 카드로 어플리케이션에 사용할 논리 채널을 열기 위한 요청 메시지를 전송하는 단계; 스마트 카드는 휴대 단말기로부터 수신한 논리 채널 열기 요청 메시지에 따라 논리 채널을 열고 그에 상응하는 응답 신

호를 휴대 단말기로 전송하는 단계; 휴대 단말기는 어플리케이션에서 사용할 논리 채널을 열어 스마트 카드와 휴대 단말기 사이의 통신 채널을 확보하는 단계를 수행한다.

<39> 이하, 본 발명에 따른 계층화 구조의 프로토콜 스택을 사용하는 스마트 카드와 휴대 단말기의 통신 환경 설정 방법에 대한 바람직한 실시 예를 첨부한 도면을 참조하여 상세하게 살펴보기로 하자.

<40> 도 2는 본 발명에 따른 계층화 구조의 프로토콜 스택을 사용하는 스마트 카드와 휴대 단말기 사이에서 통신 속도와 통신 프로토콜 및 해당 어플리케이션을 결정하는 동작 구성도이다.

<41> 본 발명에 따른 스마트 카드(100)와 휴대 단말기(200)의 구조는 도 2에 도시된 바와 같이, 전송 데이터의 송수신을 담당하는 전송 계층(120, 220)과 상기의 송수신 데이터를 처리하는 응용 계층(110, 210)이 각각 구성된다.

<42> 이러한 구성의 특징은, 멀티 어플리케이션을 지원하는 스마트 카드(100)와 휴대 단말기(200) 사이에서 어떤 어플리케이션이 통신 프로토콜을 변경하고자 할 때, 각각의 계층 사이의 독립성을 유지시켜 주는 장점이 있다.

<43> 본 발명에 따른 스마트 카드(100)와 휴대 단말기(200) 사이의 동작의 특징을 도 2를 참조하여 살펴보면, 먼저 스마트 카드(100)가 휴대 단말기(200)에 삽입되면, 휴대 단말기(200)는 스마트 카드(100)로 전원을 인가한다(S201).

<44> 휴대 단말기(200)로부터 전원이 인가되면, 스마트 카드(100)는 인가되는 전원에 따라 리셋 동작을 수행한 후, 그에 응답 신호로 자신이 지원할 수 있는 통신 환경에 대한 정보를 휴대 단말기(200)로 전송하는 것이다(S202).

<45> 휴대 단말기(200)는 상기 스마트 카드(100)로부터 전송되는 리셋 후 응답 신호를 분석 즉, 스마트 카드(100)로부터 전송되는 통신 환경에 대한 정보(예를 들면, 통신 속도, 통신 프로토콜, 전압, 전류, 데이터 보호구간 등의 정보 등)를 분석하여 해당 어플리케이션에 대한 최적의 통신 환경을 구축하고 있는지를 판단한다.

<46> 이러한 스마트 카드(100)의 통신 환경을 분석한 후, 휴대 단말기(200)는 스마트 카드(100)와의 논리 채널을 열기 위한 논리 채널 열기(OPEN) 요청 메시지를 스마트 카드(100)로 전송한다(S203).

<47> 따라서, 스마트 카드(100)는 휴대 단말기(100)로부터 수신한 논리 채널 열기 요청 메시지에 따라 휴대 단말기(200)와의 논리 채널을 열고 논리 채널 열기 요청에 대한 응답 메시지를 휴대 단말기(200)로 전송하는 것이다.

<48> 상기의 스마트 카드(100)의 응용 계층(110)은 다수의 어플리케이션(111, 112, ...)을 구비하고, 전송 계층(120)은 상기 응용 계층(110)의 다수의 어플리케이션을 지원할 수 있는 다수의 통신 환경(121, 122, ...)을 보유하고 있으며, 상기의 휴대 단말기(200)의 응용 계층(210) 역시 다수의 어플리케이션(211, 212, ...)을 보유하고 있으며, 전송 계층(220) 또한 응용 계층(210)의 어플리케이션들을 각각 지원할 수 있는 다수의 통신 환경(221, 222, ...)을 구축할 수 있다.

<49> 여기서, 하나의 어플리케이션이 하나의 통신 환경에서만 동작하는 정적인 스마트 카드 시스템과는 달리 본 발명에 따른 스마트 카드와 휴대 단말기 사이에서는 휴대 단말기의 선택에 따라 동적인 통신 환경의 설정이 가능하다.

<50> 이러한 동적인 통신 환경 설정의 특성은 하나의 응용에 대해서도 현재 어떤 서비스를 이용할 것이냐에 따라 가장 적합한 통신 환경을 재구성할 수 있는 장점이 있는 것이다.

<51> 예를 들어, 은행 접속에 스마트 카드를 사용할 경우, 현재 제 1의 어플리케이션을 이용하고 있고, 상기의 제 1의 어플리케이션 서비스 사용 중에 어떤 A 은행에 접속하여 어느 지점의 위치를 검색하고자 하는 간단한 제 2의 어플리케이션을 구동한다면, 현재 사용 중인 제 1의 어플리케이션에 영향을 미치지 않게 하기 위해 메모리 사용이 적은 T=0 프로토콜을 사용하는 통신 환경을 선택하는 것이 바람직하다.

<52> 또한, 현재 사용 중인 어플리케이션이 없고 은행 접속 후에 계좌 이체와 같은 보안성이 요구되는 데이터 전송이 필요하다면, 시큐어 메시징을 지원하는 T=1 프로토콜의 통신 환경을 설정하는 것이 바람직하다.

<53> 본 발명에 따른 휴대 단말기는 리셋 후 응답에 실려 전송되어 오는 스마트 카드 내부의 통신 환경 정보를 분석하여 통신 속도와 통신 프로토콜을 선택함으로써 상기 예에서 보인 동적인 통신 환경 설정을 수행하여 현재의 어플리케이션에 가장 적합한 통신 환경을 구축할 수 있는 것이다.

<54> 이하, 본 발명에 따른 계층화 구조의 프로토콜 스택을 사용하는 스마트 카드와 휴대 단말기의 통신 환경 설정 방법에 대하여 첨부한 도 3을 참조하여 단계적으로 살펴보기로 하자.

<55> 도 3은 본 발명에 따른 스마트 카드와 휴대 단말기의 일 실시 예에 따른 최적의 통신 환경 설정 방법에 대한 처리 동작을 설명하기 위한 흐름이다.

<56> 먼저, 휴대 단말기(200) 사용자가 스마트 카드(100)를 이용한 어플리케이션을 구동하고자 할 때, 휴대 단말기(200)에서 스마트 카드(100)에 전원을 인가한다(S301).

<57> 이어, 스마트 카드(100)는 휴대 단말기(200)에서 제공되는 전원인가에 따라 리셋 후 응답 정보를 휴대 단말기(200)로 전송하는데(S302), 여기서, 응답 정보로는 운용 전압, 전류, 데이터 보호구간 정보와 더불어 스마트 카드(100) 자신이 지원하는 통신 환경, 즉 스마트 카드(100) 자신이 지원 가능한 통신 속도와 통신 프로토콜에 대한 상세한 정보를 담고 있다.

<58> 상기 스마트 카드(100)로부터 전송되는 리셋 신호 및 응답 정보를 수신한 휴대 단말기(200)는 자신이 요구하는 리셋 후 응답 형식인지 아닌지를 판단한다(S303).

<59> 상기 판단 결과, 휴대 단말기(200)에서 요구하는 리셋 후 응답 형식이면 리셋 후 스마트 카드(100)에서 제공되는 응답 정보를 분석하여 현재 사용하고자 하는 어플리케이션에 가장 적합한 최적의 통신 환경을 설정한다(S309). 여기서, 휴대 단말기(200)에서 요구하는 응답 형식은, 운용 전압, 전류, 데이터 보호구간

정보와 더불어 스마트 카드(100)가 자신이 지원하는 통신 환경, 즉 가능한 통신 속도와 통신 프로토콜에 대한 상세한 정보를 포함하는 것이다.

<60> 최적의 통신 환경이 설정되면, 휴대 단말기(200)는 스마트 카드(100)로 어플리케이션에 사용할 논리 채널을 열기 위한 요청 메시지를 전송한다(S311).

<61> 스마트 카드(100)는 휴대 단말기(200)로부터 수신한 논리 채널 열기 요청 메시지에 따라 논리 채널을 열고 그에 상응하는 응답 신호를 휴대 단말기(200)로 전송한다(S312). 따라서, 휴대 단말기(200)는 어플리케이션에서 사용할 논리 채널을 열어 스마트 카드(100)와 휴대 단말기(200) 사이의 통신 채널을 확보하게 된다(S310).

<62> 그러나, 상기 S303 단계에서, 휴대 단말기(200)에서 요구하는 리셋 후 응답 형식이 아닌 다른 형식의 응답인 경우, 휴대 단말기(200)에서는 프로토콜/파라미터 선택 절차를 수행할 것인지를 판단하게 된다(S304).

<63> 상기 판단 결과, 휴대 단말기(200)가 프로토콜/파라미터 선택 절차를 수행하고자 하는 경우에는 스마트 카드(100)로 프로토콜/파라미터 선택 요청 메시지를 전송한다(S305).

<64> 상기 휴대 단말기(200)로부터 프로토콜/파라미터 선택 요청 메시지를 수신한 스마트 카드(100)는 스마트 카드(100) 내부에서 프로토콜/파라미터 선택 절차를 지원하는지를 판단한다(S306).

<65> 판단 결과, 스마트 카드(100)내부에서 프로토콜/파라미터 선택을 지원하지 않는 경우에는 휴대 단말기(200)로부터 다시 리셋 신호가 오기를 기다리는 리셋

대기 상태로 전환되고(S308), 반대로 프로토콜/파라미터 선택을 지원하는 경우 프로토콜/파라미터 선택 응답 메시지를 휴대 단말기(200)로 전송한다(S307).

<66> 따라서, 휴대 단말기(200)는 통신 채널을 확보할 수 있는 것이다.

<67> 한편, 상기 S304단계에서 프로토콜/파라미터 선택을 수행하지 않을 경우에는 상기 S310단계로 진행한다. 즉, 휴대 단말기(200)는 스마트 카드(100)로 어플리케이션에 사용할 논리 채널을 열기 위한 요청 메시지를 전송한다(S311). 스마트 카드(100)는 휴대 단말기(200)로부터 수신한 논리 채널 열기 요청 메시지에 따라 논리 채널을 열고 그에 상응하는 응답 신호를 휴대 단말기(200)로 전송한다(S312). 따라서, 휴대 단말기(200)는 어플리케이션에서 사용할 논리 채널을 열어 스마트 카드(100)와 휴대 단말기(200) 사이의 통신 채널을 확보하게 된다(S310).

<68> 도 3에 기초하여 전술한 일 실시 예에서 설명하였듯이 본 발명에 따른 스마트 카드와 휴대 단말기는 새로운 형식의 리셋 후 응답을 적용하여 스마트 카드와 휴대 단말기 사이에서 해당 어플리케이션에 대한 최적의 통신 환경을 구축할 수 있을 뿐만 아니라, 종래의 통신 환경도 지원할 수 있는 장점도 지니고 있다.

<69> 결국, 본 발명에 따른 계층화 구조의 프로토콜 스택을 사용하는 스마트 카드와 휴대 단말기의 통신 환경 설정 방법은, 휴대 단말기와 스마트 카드 각각의 내부에 다수의 어플리케이션과 다수의 통신 환경을 보유하며, 전송 데이터의 송수신을 담당하는 전송 계층과 상기 송수신 데이터의 처리를 담당하는 응용 계층이 구분되어 구현되어 있으며, 상기의 스마트 카드가 응답하는 리셋 후 응답은 종래의 스마트 카드가 응답하는 공지의 리셋 후 응답에 포함하는 정보와 더불어

지원 가능한 통신 환경에 대한 정보를 모두 포함하고 있기 때문에, 스마트 카드와 휴대 단말기 사이의 통신 환경을 설정하고자 하는 경우에 해당 어플리케이션에 가장 적합한 통신 환경을 동적으로 구축할 수 있는 것이다.

【발명의 효과】

<70> 이상에서 설명한 바와 같이 본 발명에 따른 계층화 구조의 프로토콜 스택을 사용하는 스마트 카드와 휴대 단말기의 통신 환경 설정 방법은, 휴대 단말기와 스마트 카드 각각의 내부에 다수의 어플리케이션과 다수의 통신 환경을 보유하며, 전송 데이터의 송수신을 담당하는 전송계층과 상기 송수신 데이터의 처리를 담당하는 응용계층이 구분되어 구현되어 있으며, 상기의 스마트 카드가 응답하는 리셋 후 응답은 종래의 스마트 카드가 응답하는 공지의 리셋 후 응답에 포함하는 정보와 더불어 지원 가능한 통신 환경에 대한 정보를 모두 포함하고 있기 때문에, 스마트 카드와 휴대 단말기 사이의 통신 환경을 설정하고자 하는 경우에 해당 어플리케이션에 가장 적합한 통신 환경을 동적으로 구축할 수 있는 것이다. 따라서, 스마트 카드를 사용하는 휴대 단말기 사용자에게 신속하고 안정적인 통신 채널을 제공할 수 있는 효과가 있다.

<71> 특히 본 발명에 따른 계층화 구조의 프로토콜 스택을 사용하는 스마트 카드와 휴대 단말기에서는 해당 어플리케이션에 대해 가장 적합한 통신 환경을 제공하기 때문에, 스마트 카드가 지니는 중요 정보의 저장과 처리 기능을 사용하고자 하는 이동 통신 시스템의 다양한 어플리케이션에 적용되어 이동 통신에서의 스마트 카드 활성화에 기여할 수 있는 효과가 있다.

【특허청구범위】

【청구항 1】

계층화 구조의 프로토콜 스택을 사용하는 스마트 카드와 휴대 단말기의 통신 환경 설정 방법에 있어서,

상기 휴대 단말기에서 스마트 카드에 전원을 인가하면, 스마트 카드는 인가되는 전원에 따라 리셋 후 응답 정보를 휴대 단말기로 전송하는 단계;

상기 스마트 카드로부터 전송되는 응답 정보가 휴대 단말기 자신이 요구한 응답 형식인 경우, 휴대 단말기는 스마트 카드에서 제공되는 응답 정보를 분석하여 현재 사용하고자 하는 어플리케이션에 가장 적합한 최적의 통신 환경을 설정하는 단계;

최적의 통신 환경이 설정되면, 휴대 단말기는 스마트 카드로 어플리케이션에 사용할 논리 채널을 열기 위한 요청 메시지를 전송하는 단계;

스마트 카드는 휴대 단말기로부터 수신한 논리 채널 열기 요청 메시지에 따라 논리 채널을 열고 그에 상응하는 응답 신호를 휴대 단말기로 전송하는 단계;

휴대 단말기는 어플리케이션에서 사용할 논리 채널을 열어 스마트 카드와 휴대 단말기 사이의 통신 채널을 확보하는 단계를 포함하는 계층화 구조의 프로토콜 스택을 사용하는 스마트 카드와 휴대 단말기의 통신 환경 설정 방법.

【청구항 2】

제1항에 있어서,

상기 스마트 카드로부터 제공되는 응답 정보는,

운용 전압, 전류, 데이터 보호구간 정보, 스마트 카드 자신이 지원하는 통신 속도, 통신 프로토콜에 대한 상세한 정보 중 적어도 하나의 정보를 포함하는 계층화 구조의 프로토콜 스택을 사용하는 스마트 카드와 휴대 단말기의 통신 환경 설정 방법.

【청구항 3】

제1항에 있어서,

상기 스마트 카드에서 제공되는 응답 형식이 휴대 단말기에서 요구하는 응답 형식이 아닌 경우,

휴대 단말기에서는 프로토콜/파라미터 선택 절차를 수행할 것인지를 판단하는 단계;

상기 판단 결과, 휴대 단말기가 프로토콜/파라미터 선택 절차를 수행하고자 하는 경우에는 스마트 카드로 프로토콜/파라미터 선택 요청 메시지를 전송하는 단계;

상기 휴대 단말기로부터 프로토콜/파라미터 선택 요청 메시지를 수신한 스마트 카드는 스마트 카드 내부에서 프로토콜/파라미터 선택 절차를 지원하는지를 판단하는 단계;

판단 결과, 스마트 카드 내부에서 프로토콜/파라미터 선택을 지원하는 경우 프로토콜/파라미터 선택 응답 메시지를 휴대 단말기로 전송하여 스마트 카드와 휴대 단말기간의 통신 채널을 확보하는 단계를 포함하는 계층화 구조의 프로토콜 스택을 사용하는 스마트 카드와 휴대 단말기의 통신 환경 설정 방법.

【청구항 4】

제1항에 있어서,

상기 스마트 카드와 휴대 단말기는,

전송 데이터의 송수신을 담당하는 전송 계층과 상기의 송수신 데이터를 처리하는 응용 계층을 각각 구비하는 계층화 구조의 프로토콜 스택을 사용하는 스마트 카드와 휴대 단말기의 통신 환경 설정 방법.

【청구항 5】

제4항에 있어서,

상기 스마트 카드와 휴대 단말기의 상기 응용 계층은, 다수의 어플리케이션을 구비하고, 상기 전송 계층은 상기 응용 계층의 다수의 어플리케이션을 지원할 수 있는 다수의 통신 환경을 보유하고 있는 계층화 구조의 프로토콜 스택을 사용하는 스마트 카드와 휴대 단말기의 통신 환경 설정 방법.

【청구항 6】

제4항 또는 제5항에 있어서,

상기 전송 계층과 응용 계층이 상호 독립적으로 구현되어 하나의 어플리케이션이 다수의 통신 프로토콜을 지원 받고, 하나의 통신 프로토콜이 다수의 어플리케이션을 지원할 수 있는 계층화 구조의 프로토콜 스택을 사용하는 스마트 카드와 휴대 단말기의 통신 환경 설정 방법.

【청구항 7】

계층화 구조의 프로토콜 스택을 사용하는 스마트 카드와 휴대 단말기의 통신 환경 설정 방법을 수행하기 위하여 디지털 처리장치에 의해 실행될 수 있는 명령어들의 프로그램이 유형적으로 구현되어 있으며, 디지털 처리장치에 의해 판독될 수 있는 기록 매체에 있어서,

상기 휴대 단말기에서 스마트 카드에 전원을 인가하면, 스마트 카드는 인가되는 전원에 따라 리셋 후 응답 정보를 휴대 단말기로 전송하는 단계;

상기 스마트 카드로부터 전송되는 응답 정보가 휴대 단말기 자신이 요구한 응답 형식인 경우, 휴대 단말기는 스마트 카드에서 제공되는 응답 정보를 분석하여 현재 사용하고자 하는 어플리케이션에 가장 적합한 최적의 통신 환경을 설정하는 단계;

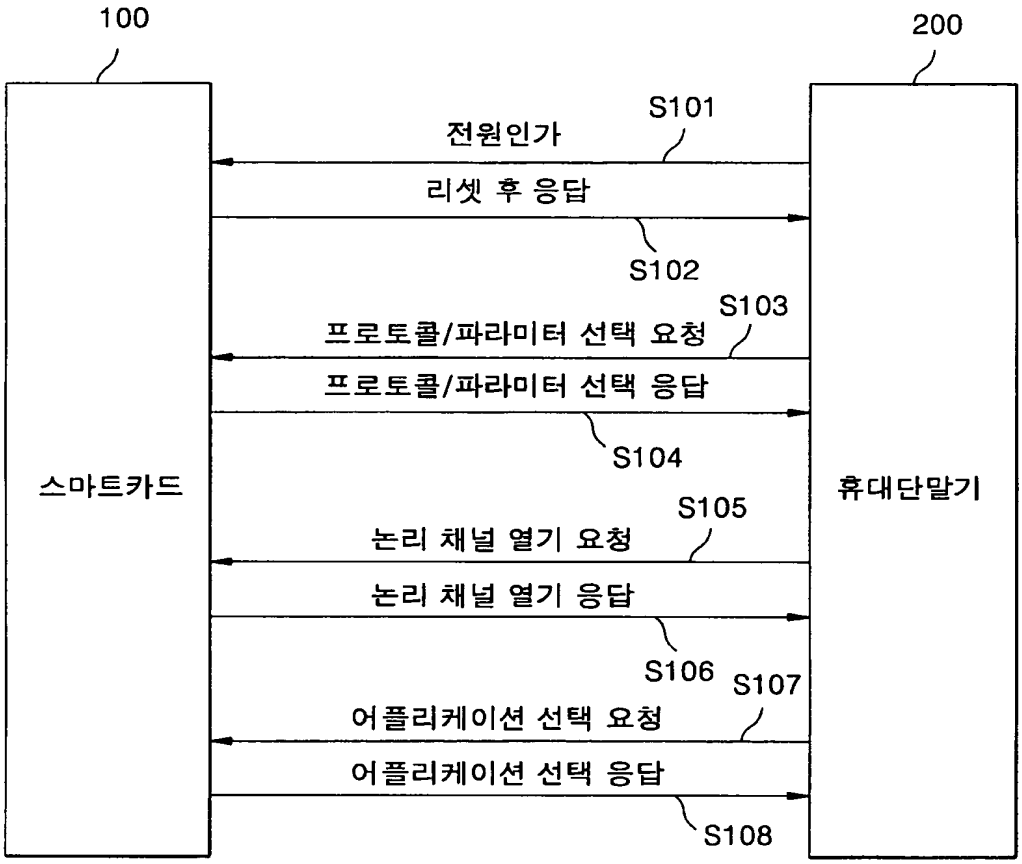
최적의 통신 환경이 설정되면, 휴대 단말기는 스마트 카드로 어플리케이션에 사용할 논리 채널을 열기 위한 요청 메시지를 전송하는 단계;

스마트 카드는 휴대 단말기로부터 수신한 논리 채널 열기 요청 메시지에 따라 논리 채널을 열고 그에 상응하는 응답 신호를 휴대 단말기로 전송하는 단계;

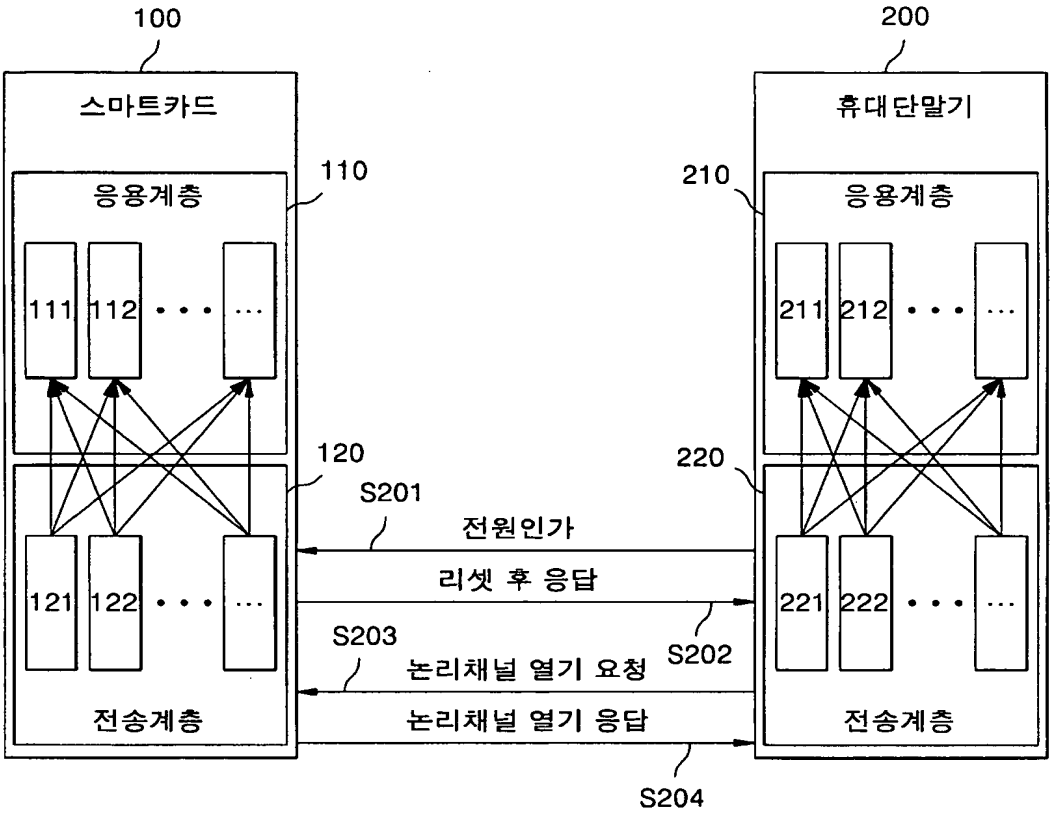
휴대 단말기는 어플리케이션에서 사용할 논리 채널을 열어 스마트 카드와 휴대 단말기 사이의 통신 채널을 확보하는 단계를 수행하는 기록 매체.

【도면】

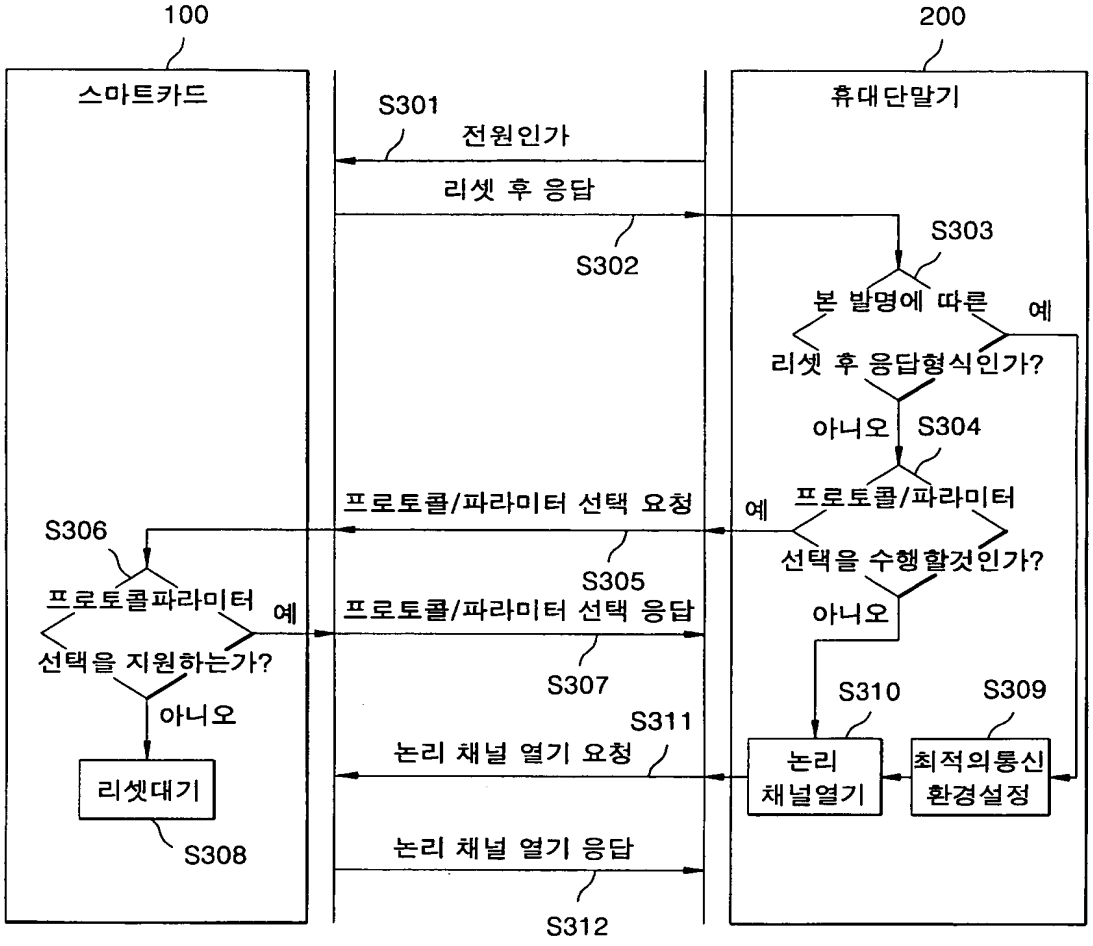
【도 1】


100
200
스마트카드
휴대단말기
S101
전원인가
리셋 후 응답
S102
S103
프로토콜/파라미터 선택 요청
프로토콜/파라미터 선택 응답
S104
S105
논리 채널 열기 요청
논리 채널 열기 응답
S106
S107
어플리케이션 선택 요청
어플리케이션 선택 응답
S108

【도 2】


100
스마트카드
110
응용계층
111
112
120
121
122
전송계층
200
휴대단말기
210
응용계층
211
212
220
221
222
전송계층
S201
전원인가
리셋 후 응답
S202
S203
논리채널 열기 요청
논리채널 열기 응답
S204

【도 3】


100
200
스마트카드
휴대단말기
S301
전원인가
리셋 후 응답
S302
S303
본 발명에 따른
예
리셋 후 응답형식인가?
아니오
S304
프로토콜/파라미터
선택을 수행할것인가?
예
프로토콜/파라미터 선택 요청
S305
S306
프로토콜파라미터
선택을 지원하는가?
예
프로토콜/파라미터 선택 응답
S307
아니오
리셋대기
S308
S310
S309
S311
논리 채널 열기 요청
논리 채널열기
최적의통신 환경설정
논리 채널 열기 응답
S312

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.		(11) 공개번호	특1999-019525
G06K 19/07		(43) 공개일자	1999년03월15일
(21) 출원번호	특1997-042908		
(22) 출원일자	1997년08월29일		
---	---
(71) 출원인	엘지전자 주식회사, 구자홍 대한민국 150-010 서울특별시 영등포구 여의도동 20번지
(72) 발명자	장복현 대한민국 137-010 서울특별시 서초구 양재동 106-9 신우주택 204
(74) 대리인	김용인 심창섭
---	---
(77) 심사청구	없음

(54) 출원명 스마트(smart)카드 저장데이터 수신방법

요약

대량의 데이터 전송시 전송속도를 향상시킬 수 있도록 한 스마트카드의 저장데이터 수신방법에 관한 것으로, 스마트카드에서 전송된 데이터를 수신하는 방법에 있어서, 통신모드를 판단하는 단계, 판단결과에 따른 통신모드로 데이터 수신이 가능하도록 통신라인을 전환하는 단계, 전환된 통신라인을 통해 스마트카드에 저장된 데이터를 수신하는 단계를 포함하여 이루어지므로 데이터 전송효율 및 데이터 처리성능을 향상시킬 수 있다.

대표도

도3

명세서

도면의 간단한 설명

도 1은 종래의 기술에 따른 스마트카드 저장데이터 수신장치를 나타낸 블록도

도 2는 본 발명에 따른 스마트카드 저장데이터 수신장치를 나타낸 블록도

도 3은 본 발명에 따른 스마트카드 저장데이터 수신방법을 나타낸 플로우챠트

* 도면의 주요부분에 대한 부호의 설명

10: 스마트카드 20: 호스트장치

30, 40: 스마트카드 데이터 수신장치 31, 41: 전원부

32, 42: 클럭발생부 33, 43: 제어부

34, 44: 스마드카드 인터페이스부 35: UART

36, 46: 송수신버퍼 37, 47: 호스트 인터페이스부

45: GPI/O

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 스마트카드에 관한 것으로서, 특히 스마트카드 저장데이터 수신방법에 관한 것이다.

일반적으로 스마트카드는 사용자 인식을 위한 고유데이터를 비롯하여 각종 데이터를 내장한 집적회로가 인쇄된 카드로 신원을 확인하기 위한 출입증 또는 휴대용 통신단말기에 사용자의 개인데이터 및 통신관련 데이터를 입력시키기 위하여 사용되고 있다. 그리고 현재사회가 데이터 통신사회로 변모하고 계속 발전해감에 따라 스마트카드의 사용범위가 확대되고 그에 따라 스마트카드에 저장되는 데이터의 종류 및 양이 급속히 증가하고 있다. 특히, 통신면에서 음성 및 문자는 물론이고 영상통신이 발전해감에 따라 단말장치 등에서 사용되는 LCD 화면의 사이즈도 증가하므로 기본적인 개인 고유데이터 즉 문자데이터는 물론이고 예를 들어 자신의 얼굴 즉 화상데이터를 동영상으로 스마트카드에 저장하는 등의 변화는 필연적이라 할 수 있다. 따라서 스마트카드에 저장되는 데이터의 양도 큰폭으로 증가할 것이므로 기존의 기술을 이용할 경우 스마트카드에 저장된 대량의 데이터를 읽어들이는 속도 측면에서 속도증가의 필요성이 당면과제로 대두될 것은 명백하다.

이하, 종래의 기술에 따른 스마트카드 저장데이터 수신방법을 첨부한 도면을 참조하여 설명하면 다음과 같다.

도 1은 종래의 기술에 따른 스마트카드 저장데이터 수신장치를 나타낸 블록도로써, 스마트카드 데이터 수신장치(30)는 동작전원(Vcc, Vpp)을 공급하는 전원부(31), 일정 클럭(Clock)을 발생시키는 클럭발생부(32), 인터페이스 동작을 제어하고 제어신호를 출력하는 제어부(33), 스마드카드(10)에 전원부(31)의 동작전원, 클럭발생부(32)의 클럭 및 제어부(33)의 리셋신호를 제공하고 스마드카드(10)의 데이터교환을 수행하기 위한 스마트카드 인터페이스부(34), 상기 스마트카드 인터페이스부(34)를 통해 직렬형태로 입력된 스마드카드(10)의 데이터를 제어부(33)에 입력가능한 데이터 형태로 처리하여 직렬 I/O버스를 통해 제어부(33)에 전송하는 UART(Universal Asynchronous Receiver/Transmitter: 범용비동기 송/수신기)(35), 상기 UART(35)에서 출력된 데이터를 임시저장하여 출력하는 송수신버퍼(36), 제어부(33)와 호스트장치(20)의 데이터교환을 위한 호스트 인터페이수부(37)로 구성된다. 이때 스마드카드(10)는 도 1에서 도시생략된 단자를 포함하여 6개의 단자 즉, Vcc, Vpp, 클럭(Clock), 리셋(Reset), 접지 및 직렬 I/O단자를 구비한다.

이와 같이 구성된 스마트카드 저장데이터 수신장치의 데이터 수신동작을 살펴보면 다음과 같다.

먼저, 스마드카드(10)는 스마트카드 인터페이스부(34)를 통해 전원 및 신호전송용 클럭을 제공받고 저장된 데이터를 직렬통신라인을 통해 UART(35)로 출력한다.

이때 스마드카드(10)에 저장된 데이터는 주로 사용자의 고유정보 또는 상기 고유정보에 상응하는 통신관련 데이터 등의 문자 데이터이다.

이어서 UART(35)는 전송된 데이터를 입력레지스터를 통해 입력받고 콘트롤레지스터에 저장된 데이터포멧에 따라 패리티 비트(Parity bit) 또는 아이디 비트(ID bit) 등을 첨가하여 제어부(33)에서 판독가능한 데이터로 변화처리하고 출력레지스터를 통해 출력한다. 그리고 상기 UART(35)에서 출력된 데이터는 송수신버퍼(36)를 경유하여 제어부(33)에 입력된다. 이어서 제어부(33)는 호스트 인터페이수부(37)를 통해 이루어지는 호스트장치(20)와의 데이터 전송동작을 제어한다.

발명이 이루고자 하는 기술적 과제

종래의 기술에 따른 스마트카드는 개인정보 등 소량의 문자데이터가 저장되므로 직렬통신방법을 이용하여 데이터를 전송하였으나 화상데이터 등 문자데이터에 비해 대량의 데이터를 직렬통신을 이용하여 전송하면 전송속도가 큰 폭으로 저하되므로 이를 적용한 시스템의 데이터 처리성능이 저하되는 문제점이 있다.

따라서 본 발명은 상기한 종래의 문제점을 해결하기 위하여 안출한 것으로서; 대량의 데이터 전송시 전송속도를 향상시킬 수 있도록 한 스마트카드의 저장데이터 수신방법을 제공함에 그 목적이 있다.

발명의 구성 및 작용

본 발명은 통신모드를 판단하는 단계, 판단결과에 따른 통신모드로 데이터 수신이 가능하도록 통신라인을 전환하는 단계, 전환된 통신라인을 통해 스마트카드에 저장된 데이터를 수신하는 단계를 포함하여 이루어짐을 특징으로 한다.

이하, 첨부된 도면을 참조하여 본 발명에 따른 스마트카드 저장데이터 수신방법을 설명하면 다음과 같다.

도 2는 본 발명에 따른 스마트카드 저장데이터 수신장치를 나타낸 블록도이고, 도 3은 본 발명에 따른 스마트카드 저장데이터 수신방법을 나타낸 플로우차트이다.

본 발명에 따른 스마트카드 저장데이터 수신장치는 일부구성을 제외하고는 종래의 기술과 동일하므로 상세한 구성설명은 생략하기로 한다.

도 2에 도시된 바와 같이, 스마트카드 저장데이터 수신장치(40)는 전원부(41), 클럭발생부(42), 인터페이스 동작을 제어하고 제어신호를 출력하는 제어부(43), 스마드카드(10)에 전원부(41)의 동작전원, 클럭발생부(42)의 클럭 및 제어부(43)의 리셋신호를 제공하고 스마드카드(10)의 데이터교환을 수행하기 위한 스마트카드 인터페이스부(44), 상기 스마트카드 인터페이스부(34)를 통해 병렬형태로 입력된 스마드카드(10)의 데이터를 제어부(43)에 입력가능한 데이터 형태로 처리하고 병렬 I/O버스를 통해 제어부(43)에 전송하는 GPI/O(General Purpose Input/Output: 범용입출력회로)(45), 상기 GPI/O(45)에서 출력된 데이터를 임시저장하여 출력하는 송수신버퍼(46), 제어부(43)와 호스트장치(20)의 데이터교환을 위한 호스트 인터페이수부(47)로 구성된다.

이때 스마드카드(10)는 종래의 6개의 단자 즉, Vcc, Vpp, 클럭(Clock), 리셋(Reset), 접지 및 I/O단자 이외에 4bit 또는 8bit 즉, 4개 또는 8개의 병렬 I/O단자를 더 구비한다. 그리고 스마트카드 인터페이스부(44)의 단자수도 상기 스마드카드(10)의 병렬단자수에 따라 가변되고, GPI/O(45)에서 송수신버퍼(46)를 경유하여 제어부(43)에 이르는 버스라인도 상기 스마드카드(10)의 병렬 I/O단자수에 상응하는 병렬 I/O버스라인으로 전환된다.

이와 같이 구성된 스마트카드의 저장데이타 수신장치의 데이터 수신방법을 도 3의 플로우챠트를 참조하여 설명한다.

먼저, 제어부(43)는 스마트카드신호가 입력되는지 즉, 사용자가 스마드카드(10)를 휴대전화 등의 단말기에 장착하는지 여부를 판단한다(S29). 그리고 그 판단결과(S29), 스마드카드(10)가 단말기에 장착되면 스마드카드(10)는 스마트카드 인터페이스부(44)를 통해 전원 및 데이터전송용 클럭을 제공받고 데이터전송을 개시한다. 이어서 스마드카드(10)에서 전송된 스마트카드 인터페이스부(44)를 경유하고 I/O 버스라인을 통해 GPI/O(45)로 입력된다. 그리고 GPI/O(45)는 전송된 데이터를 일정 데이터포멧에 따라 패리티 비트(Parity bit) 또는 아이디 비트(ID bit) 등을 첨가하고 제어부(43)에서 읽을 수 있는 데이터로 변화처리하여 출력한다. 이어서 GPI/O(45)에서 출력된 데이터는 송수신버퍼(46)를 경유하여 제어부(43)로 전송된다.

한편, 제어부(43)는 데이터 통신모드가 병렬통신모드인지 여부를 판단한다(S12).

이때 상술한 바와 같이 통신기술의 발전과 다변화에 따라 스마드카드(10)에 동영상 등의 화상데이터를 저장해야할 경우 데이터 전송속도향상을 위하여 병렬통신방식에 의해 데이터가 전송되어야한다. 따라서 병렬통신방식을 통해 통신을 수행함은 물론이고 현재의 직렬통신방식에도 적용할 수 있도록 제어부(43)의 알고리즘내에 통신모드판단을 저장하는 것이다. 또한 통신모드판단은 연결된 I/O 버스가 직렬인지 또는 병렬인지를 판단하는 것이다.

그리고 그 판단결과(S12), 통신모드가 직렬이면 연결된 직렬 I/O 버스를 통해 스마드카드(10)의 데이터를 직렬수신할 수 있도록 I/O 라인을 제어하고 통신가능상태로 전환하여 스마드카드(10)로 부터 전송되는 데이터를 수신하고(S13), 통신모드가 병렬이면 연결된 병렬 I/O 버스를 통해 스마드카드(10)의 데이터를 병렬수신할 수 있도록 I/O 라인을 제어하고 통신가능상태로 전환하여 스마드카드(10)에서 전송되는 데이터를 수신한다(S14). 이어서 데이터수신이 완료되었는지 여부를 판단하여(S15), 스마드카드(10)로 부터의 데이터 송신이 완료될 때까지 현재 사용중인 병렬 또는 병렬 I/O 버스를 통해 데이터수신을 계속 수행한다(S16).

발명의 효과

본 발명에 따른 스마트카드의 저장데이터 수신방법은 다음과 같은 효과가 있다.

첫째, 스마트카드에 저장된 데이터를 전송받을 때 직렬통신방식 및 병렬통신방식을 상호보완하여 적용하므로 기존의 기술은 물론이고 다변화되어가는 통신기술에 대한 호환성이 우수하다.

둘째, 동영상 등 대량의 데이터 전송시 병렬통신방식을 적용하므로 병렬통신방식을 적용하는것에 비해 데이터 전송속도가 현격히 증가하여 데이터 전송효율 및 데이터 처리효율을 향상시킬 수 있다.

(57) 청구의 범위

청구항 1.

스마트카드에서 전송된 데이터를 수신하는 방법에 있어서,

통신모드를 판단하는 단계;

상기 판단결과에 따른 통신모드로 데이터 수신이 가능하도록 통신라인을 전환하는 단계;

상기 전환된 통신라인을 통해 스마트카드에 저장된 데이터를 수신하는 단계를 포함하여 이루어짐을 특징으로 하는 스마트카드 저장데이터 수신방법.

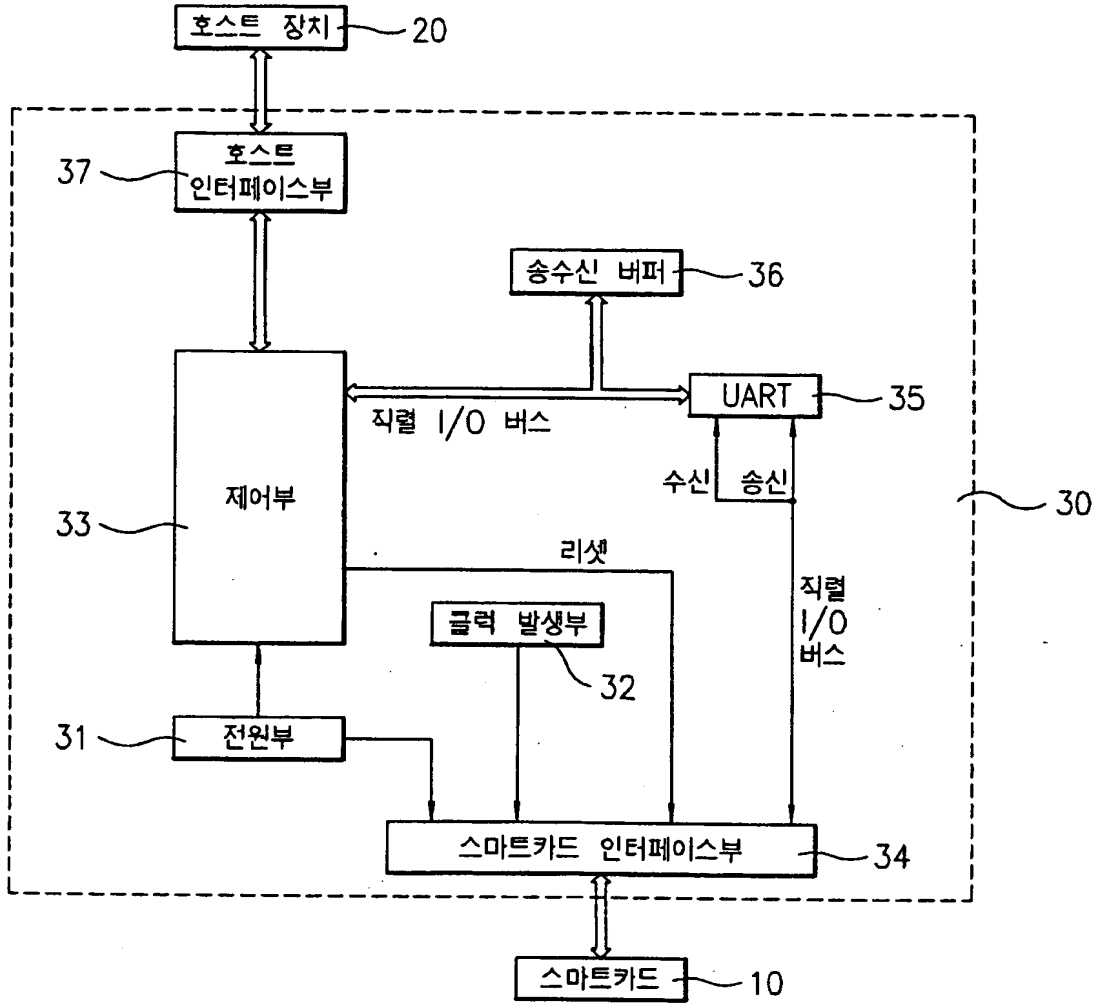
청구항 2.

제 1 항에 있어서,

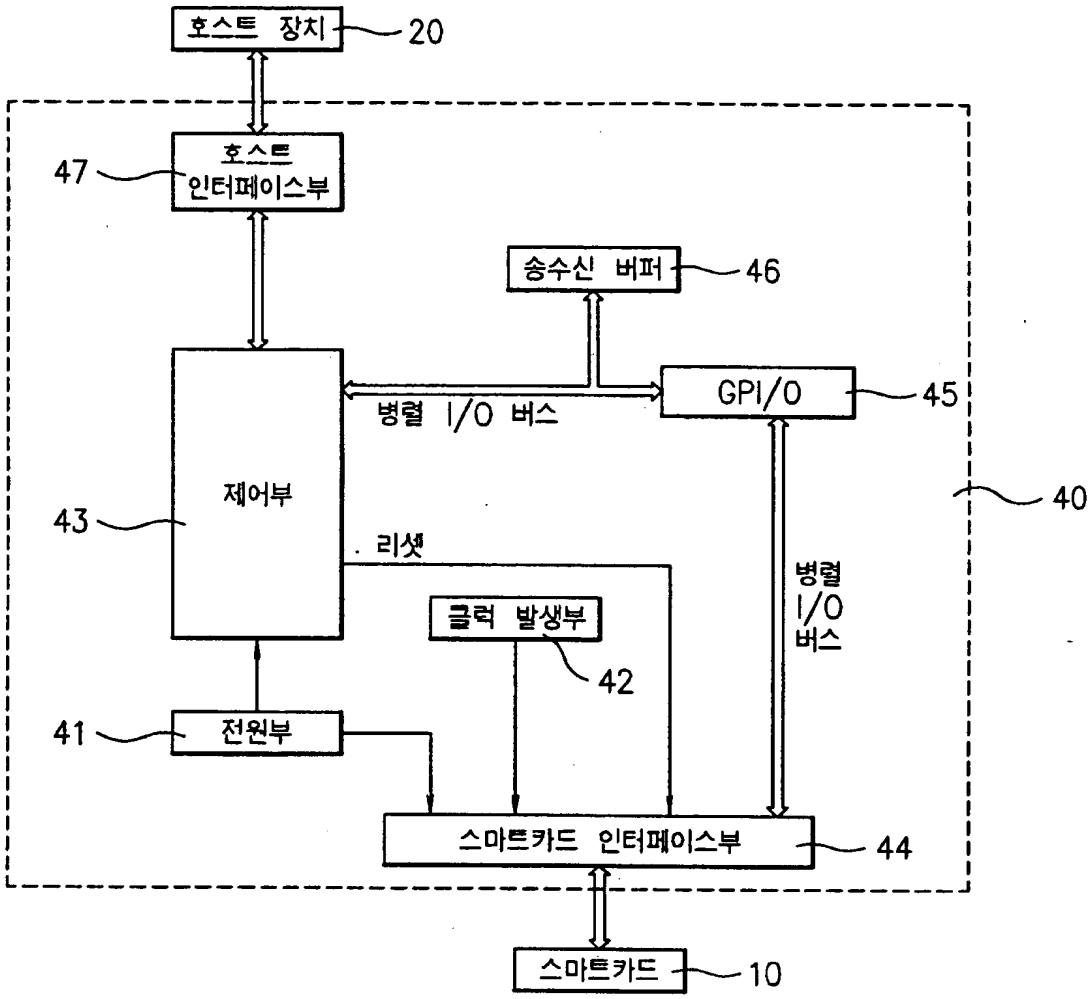
상기 통신모드 판단단계는 직렬통신모드 또는 병렬통신모드를 판단하는 단계임을 특징으로 하는 스마트카드 저장데이터 수신방법.

도면

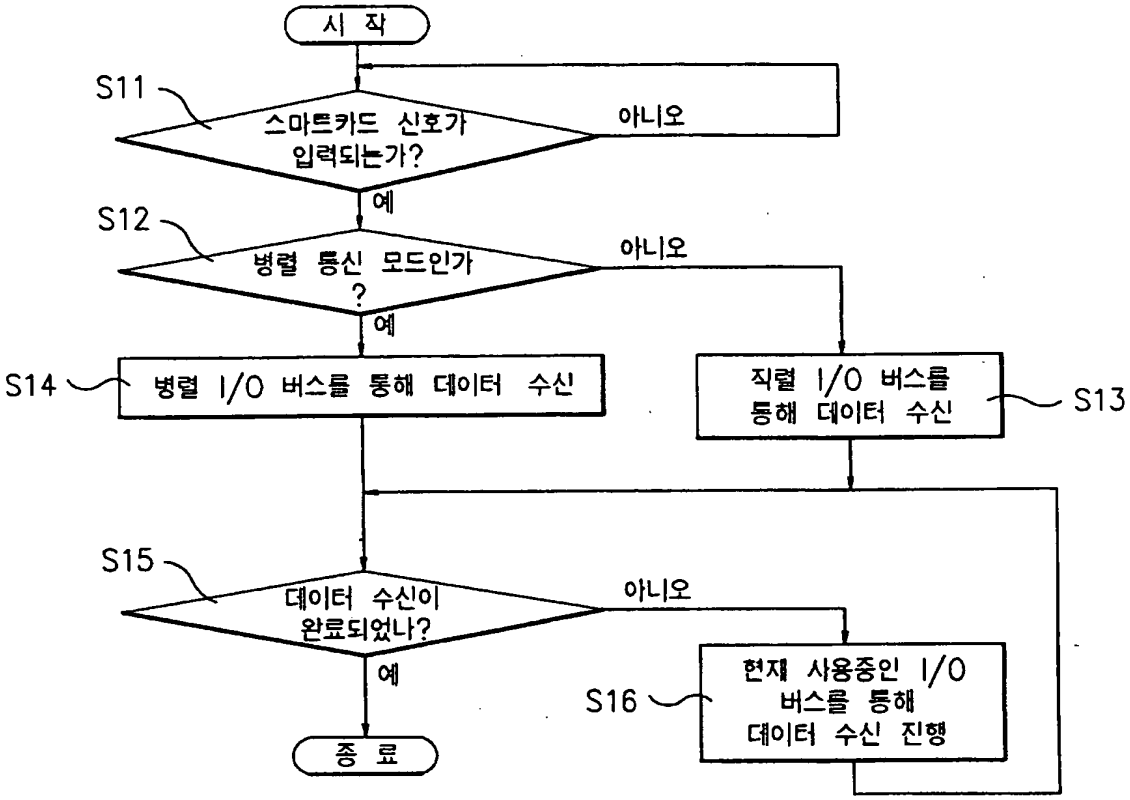
도면 1


호스트 장치
20
호스트
인터페이스부
37
송수신 버퍼
36
UART
35
직렬 I/O 버스
수신
송신
제어부
33
30
리셋
직렬
I/O
버스
클럭 발생부
32
전원부
31
스마트카드 인터페이스부
34
스마트카드
10

도면 2


호스트 장치
20
호스트
인터페이스부
47
송수신 버퍼
46
병렬 I/O 버스
GPI/O
45
제어부
43
40
리셋
병렬
I/O
버스
글럭 발생부
42
41
전원부
스마트카드 인터페이스부
44
스마트카드
10

도면 3


시 작
S11
스마트카드 신호가 입력되는가?
아니오
예
S12
병렬 통신 모드인가 ?
아니오
예
S14
병렬 I/O 버스를 통해 데이터 수신
직렬 I/O 버스를 통해 데이터 수신
S13
S15
데이터 수신이 완료되었나?
아니오
예
S16
현재 사용중인 I/O 버스를 통해 데이터 수신 진행
종 료

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl. G06K 19/07		(11) 공개번호	특2000-0000644
		(43) 공개일자	2000년01월15일
(21) 출원번호	10-1998-0020386		
(22) 출원일자	1998년06월02일		
---	---
(71) 출원인	두평수 대한민국 573430 전라북도 군산시 사정동 421번지 금호타운아파트105-103
(72) 발명자	두평수 대한민국 573-430 전라북도 군산시 사정동 421번지 금호타운아파트 105-103
(74) 대리인	김영철
---	---
(77) 심사청구	있음

(54) 출원명 다용도 접촉식 IC카드 단말기 및 그 제어방법

요약

본 발명은 다용도 접촉식 IC카드 단말기 및 그 제어방법에 관한 것으로, IC카드가 삽입되어 접점이 연결되면 이를 감지한 마이크로콘트롤러에서는 IC카드에 전원과 리셋 신호 및 클럭 신호를 각각 공급하도록 IC카드 인터페이스부에 내장된 각각의 회로들을 제어하고 통신용 단자를 단말기에 연결시키게 된다. 만약, IC카드가 단말기에 연결이 되지 않거나, 통신 중 오류가 발생되면 마이크로콘트롤러는 이를 감지하여 IC카드 인터페이스에 내장된 각각의 회로들을 제어하여 IC카드로 공급되는 전원과 리셋 신호 및 클럭 신호의 발생을 차단시키게 된다. IC카드가 연결이 되어 전원과 리셋 신호 및 클럭 신호가 입력되면, IC 카드는 필요한 정보의 신호를 단말기로 전송하게 되며, 이 전송된 신호를 수신한 마이크로콘트롤러에서는 필요한 프로토콜을 설정하게 된다. 이때, 본 발명의 IC카드 단말기는 단말기와 IC카드간에 필요한 정보 교환으로 카드내의 필요한 영역에 있는 데이터를 갱신할 수 있다. 또한 IC카드의 남은 금액이나 도수가 한계치에 도달할 때 이를 표시 장치를 통하여 사용자에게 알려주고, 필요시 수도·가스·전기 등의 계량기에 연결된 차단설비를 동작시켜 공급을 차단시키거나 자동차의 동작을 제어할 수 있다.

대표도

도1

명세서

도면의 간단한 설명

도 1 은 본 발명에 의한 접촉식 IC카드 단말기의 블록구성도

도 2 는 본 발명에서 사용된 마이크로 콘트롤러의 동작 흐름도

* 도면의 주요 부분에 대한 부호의 설명 *

110 : IC카드 인터페이스부 120 : 전원 공급부

130 : 표시부 140 : 신호 입력부

150 : 발진부 160 : 출력 인터페이스부

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 다용도 접촉식 IC카드 단말기 및 그 제어방법에 관한 것으로, 특히 개인용 컴퓨터나 전화회선에 연결하지 않고도 독립적으로 전기·수도·가스·열량계 등의 각종 계량기나 자동차의 속도센서 및 엔진, 그리고 여러 가지 의료용 센서와 연결하여 사용량이나 자동차의 운행거리에 따라 요금이나 세금 등을 정산할 수 있고, 의료용의 각종 센서의 정보를 처리하여 기억할 수 있는 다용도 접촉식 IC카드 단말기 및 그 제어방법에 관한 것이다.

1974년 프랑스의 R.MOREN에 의하여 접촉식 IC카드(contact IC card or smart card)가 특허출원 된 이후 유럽을 중심으로 자기띠(magnet strip e) 방식의 신용카드와 같은 각종 카드들이 점차적으로 IC카드로 대체되기 시작하였다. 이 IC카드는 발달된 컴퓨터 통신과 결합하여 전자화폐, 신분확인, 건물의 보안장치, 개인용 컴퓨터의 보안장치, 공중전화용 카드 등에 응용되고 있다.

접촉식 IC카드 단말기들도 응용분야에 적합하도록 개인용 컴퓨터와 직렬통신 방식인 RS-232나 RS-422,423과 같은 방식으로 연결하여 개인용 컴퓨터에 있는 응용 프로그램을 동작시켜 연산을 행한다.

이때, 전자화폐의 경우에는 온 라인(on-line)이나 오프 라인(off-line) 방식으로 해당 은행으로 전송함으로써 금액이 취급점포 계좌로 이체되고, 보안 시스템의 경우에서는 사용자가 출입문에 설치된 단말기에 ID카드를 넣으면 이를 주컴퓨터에서 확인을 한 후 출입문의 개폐 여부를 결정하게 된다.

그리고, 개인용 컴퓨터의 경우에는 카드에 내장된 ID를 이용 본인을 확인하여 컴퓨터의 키보드나 하드디스크 등을 구동하도록 하는 방식을 사용하며, 공중전화에서도 통화가 접속되면 회선의 극성이 바뀌면서 해당액을 감액하도록 하는 방식들을 사용하고 있다.

발명이 이루고자 하는 기술적 과제

그런데, 이와 같이 구성된 종래의 접촉식 IC카드 단말기에 있어서는, IC카드 단말기를 개인용 컴퓨터나 전화회선에 연결해서 사용하기 때문에 휴대가 곤란한 문제점이 있었다.

따라서, 본 발명은 상기 문제점을 해결하기 위하여 이루어진 것으로, 본 발명의 목적은 개인용 컴퓨터나 전화회선에 연결하지 않고도 독립적으로 전기·수도·가스·열량계 등의 각종 계량기나 자동차의 속도센서 및 엔진, 그리고 여러 가지 의료용 센서와 연결하여 사용량이나 자동차의 운행거리에 따라 요금이나 세금 등을 정산할 수 있고, 의료용의 각종 센서의 정보를 처리하여 기억할 수 있는 다용도 접촉식 IC카드 단말기 및 그 제어방법을 제공하는데 있다.

발명의 구성 및 작용

상기 목적을 달성하기 위하여, 본 발명의 다용도 접촉식 IC카드 단말기 제어방법에 있어서,

상기 단말기와 IC카드의 접점이 연결되었는지 확인하는 과정과,

상기 IC카드의 접점 연결을 확인한 후, IC카드에 전원·리셋 신호·클럭 신호를 공급하고 통신용 단자를 단말기에 연결시키는 과정과,

상기 IC카드의 접점이 연결되지 않거나 통신 중 오류가 발생시 카드 인터페이스에서 공급하는 전원과 클럭 및 I/O를 차단시키고, 모든 동작을 처음으로 피드백시키는 과정과,

상기 리셋 신호를 공급받은 후 IC카드에서 보내는 신호를 수신하는 과정과,

상기 수신된 신호에 포함된 각 종 정보에 따라 단말기와 카드간에 전송시 필요한 프로토콜을 설정하는 과정과,

상기 단말기와 IC카드간에 응용에 필요한 정보를 교환하고 센서에서 입력된 아날로그나 디지털 신호들을 금액 또는 도수로 변환하여 카드내의 필요한 영역에 있는 데이터를 갱신하는 과정과,

갱신금액 또는 도수가 한계치에 도달할 때에는 표시장치를 통하여 사용자에게 알려주고 필요시 엔진이나 계량기에 연결된 차단설비를 동작시키는 신호를 출력하는 과정을 구비한 것을 특징으로 한다.

상기 목적을 달성하기 위하여, 본 발명의 다용도 접촉식 IC카드 단말기는,

IC카드와 단말기를 연결하기 위한 콘넥터와, 상기 IC카드에 전원을 공급하는 전원회로부와, 상기 IC카드에 클럭/리셋 신호를 각각 발생시키는 클럭/리셋 신호발생회로부와, 마이크로콘트롤러의 출력단자에 연결하여 이들을 제어 할 수 있는 논리회로부로 구성된 IC카드 인터페이스 수단과,

자동차의 회전센서 또는 전기·수도·가스등의 계량장치나 의료용 센서에서 오는 아날로그 신호나 디지털 신호를 입력받아 단말기에 연결하여주는 회로로서, 각종 센서에서 유입되는 전압과 전류를 마이크로콘트롤러에 알맞는 전압과 전류로 정합하는 인터페이스 회로부를 포함하는 신호입력수단과,

상기 IC카드의 사용자·잔여금액·장치번호 등의 정보를 표시하며, 잔여금액이 일정치 이하로 내려갈 경우 이를 소리로 울려서 알리는 표시 및 경보 수단과,

상기 IC카드와 단말기에서 처리된 금액에 따라 해당된 전기·수도·가스등을 차단하거나 자동차의 동작을 제어하는 부분으로, 각 장치의 전기적 특성을 정합시키기 위한 인터페이스 회로부를 포함하는 출력 인터페이스 수단과,

상기 IC카드 인터페이스 수단, 신호입력수단, 표시 수단, 출력 인터페이스 수단의 동작을 제어하는 마이크로콘트롤러와,

상기 마이크로콘트롤러를 동작시키기 위해서 필요한 클럭신호를 발생시키는 발진 수단과,

상기 마이크로콘트롤러나 IC카드 인터페이스 수단, 출력 인터페이스 수단, 표시 수단, 신호입력수단에서 사용할 직류전압을 공급하는 전원공급수단을 구비하여 이루어진 것을 특징으로 한다.

이하, 본 발명의 일실시예에 관하여 첨부도면을 참조하면서 상세히 설명한다.

도 1은 본 발명에 의한 접촉식 IC카드 단말기의 블록구성도로서, 마이크로 콘트롤러(100), IC카드 인터페이스부(110), 전원 공급부(120), 표시부(130), 신호 입력부(140), 발진부(150), 출력 인터페이스부(160)로 구성된다.

상기 IC카드 인터페이스부(110)는 IC카드와 단말기를 연결하기 위한 콘넥터와, 상기 콘넥터에 IC카드가 삽입시 전원을 공급하는 전원(Vcc) 공급부와, 상기 IC카드가 활성화 되었을 때 상기 IC카드로 클럭 및 리셋 신호를 발생시키는 클럭/리셋 신호발생회로부와, 마이크로콘트롤러의 출력단자에 연결되어 상기 IC카드로 전원공급과 클럭 및 리셋 신호의 공급을 제어하는 논리회로로 구성된다.

상기 IC카드 인터페이스부(110)로 IC카드가 삽입되어 접점이 연결되면, 마이크로콘트롤러(100)에 의해 상기 IC카드에 전원, 리셋 신호, 클럭 신호 등을 공급하는 역할을 한다.

상기 전원 공급부(120)는 마이크로콘트롤러(100)나 IC카드 인터페이스부(110), 출력 인터페이스부(160), 표시부(130), 신호 입력부(140)에서 사용할 직류전압(5V와 12V)를 공급한다.

상기 표시부(130)는 엘이디(LED)를 사용하여 카드내의 잔여금액에 따라 점멸속도를 다르게 하여 표시하거나, 엘씨디(LCD)를 이용하여 문자로 사용자, 잔여금액, 장치번호 등의 정보를 표시토록하며 부저를 통해 소리를 발생케 한다.

상기 신호 입력부(140)는 자동차의 회전센서, 또는 전기·수도·가스등의 계량장치나 의료용 센서에서 오는 아날로그나 디지털 입력을 받아 단말기에 연결하여주는 회로로서, 각종 센서에서 유입되는 전압과 전류를 마이크로콘트롤러에 알맞는 전압과 전류로 정합하는 인터페이스 회로를 포함한다.

상기 발진부(150)는 마이크로콘트롤러(100)를 동작시키기 위해서 필요한 클럭신호를 발생시키는 회로로서, 정확한 발진이 되도록 4Mhz의 크리스탈 발진자를 사용한다.

상기 출력 인터페이스부(160)는 IC카드와 단말기에서 처리된 금액에 따라 해당된 전기·수도·가스등을 차단하거나 자동차를 정지시키기 위해 계량기의 릴레이, 밸브 기타 전자회로와 자동차의 ECU(Electronic Control Unit)나 연료분사 밸브에 연결하여 연료 주입을 차단하는 신호를 발생시키는 부분으로, 각 장치의 전기적 특성을 정합시키기 위해 릴레이나 포토커플러, 오픈 콜렉터(open collecter), 오픈 드레인(open drain)과 같은 기법의 인터페이스 회로를 포함한다.

상기 마이크로콘트롤러(100)는 A/D변환기와 카운터, 직렬통신기능 및 입출력 포트를 가진 마이크로콘트롤러로서, 빠른 동작을 위해 RISC 구조와 메모리 카드를 위하여 I^2C 규격도 지원하는 형을 사용한다.

일반적으로, IC카드 단말기가 세계적으로 통용되고 있는 기존의 IC카드들을 그대로 활용하기 위해서는 ISO 7816규정을 만족하여야 한다.

그러므로, 본 발명에 의한 접촉식 IC카드 단말기에서 사용하는 프로그램은 ISO 7816 규정을 만족하도록 발명하였다.

본 발명의 접촉식 IC카드 단말기에서 사용한 프로그램의 흐름도를 도 2에 나타내었다.

상기 흐름도에서 각 서브루틴들은 다음과 같은 기능을 수행한다.

1) 카드 삽입 확인(제 220 단계) : 단말기와 IC카드의 접점이 연결되었는지 확인하는 과정으로 마이크로콘트롤러(100)는 콘넥터에 있는 보조접점의 신호를 확인하여 판정한다.

2) 접점의 활성화(제 230 단계) : 접점 연결을 확인한 후 단말기는 IC카드에 전원, 리셋 신호, 클럭 신호를 공급하고 통신용 단자(I/O)를 단말기에 연결시키는 과정으로, 마이크로콘트롤러(100)는 IC카드 인터페이스부(110)에 포함된 논리회로에 필요한 신호를 공급한다.

3) 접점의 비활성화(제 240 단계) : IC카드에 가해지는 전기적인 충격을 방지하여 기억된 정보를 보호하기 위해서 접점이 연결되지 않거나 통신 중 오류가 발생하면 카드 인터페이스에서 공급하는 전원과 클럭, I/O를 차단시키는 과정으로서, 마이크로콘트롤러(100)는 IC카드 인터페이스부(110)에 포함된 논리회로에 차단 신호들을 보낸다.

4) ATR(answer to reset) 수신(제 250 단계) : IC카드 인터페이스부(110)에서 공급한 리셋 신호를 받은 IC카드는 400~40,000 클럭 내에 ATR 신호를 단말기로 보내야 하는데, 카드에서 보내는 이 신호를 수신하는 단계이다.

5) PTS(Protocol type selection)(제 260 단계) : ATR에 포함된 각 종 정보에 따라 단말기와 카드간에 전송시 필요한 프로토콜을 설정하는 단계이다.

6) 통신과 연산(제 270 단계) : 단말기와 IC카드간에 응용에 필요한 정보를 교환하고 센서에서 입력된 아날로그나 디지털 신호들을 금액 또는 도수로 변환하여 카드내의 필요한 영역에 있는 데이터를 갱신한다. 또한, 금액이나 도수가 한계치에 도달할 때에 표시장치를 통하여 사용자에게 알려주며, 필요시 엔진이나 계량기에 연결된 차단설비를 동작시키는 신호를 출력인터페이스에 공급하는 단계이다. 그리고 정보의 보호를 위하여 각종 암호 및 복호과정이 포함된다.

결론적으로, 본 발명에 의한 접촉식 IC카드 단말기에서는, IC카드 인터페이스부(110)에 IC카드가 삽입되어 접점이 연결되면, 이를 감지한 마이크로콘트롤러(100)에서는 상기 IC카드에 전원과 리셋 신호 및 클럭 신호를 각각 공급하도록 IC카드 인터페이스부(110)에 내장된 각각의 회로들을 제어하고, 통신용 단자를 단말기에 연결시키게 된다.

만약, IC카드가 단말기에 연결이 되지 않거나, 통신 중 오류가 발생되면 마이크로콘트롤러는 이를 감지하여 IC카드 인터페이스부(110)에 내장된 각각의 회로들을 제어하여 IC카드로 공급되는 전원과 리셋 신호 및 클럭 신호의 발생을 차단시키게 된다.

IC카드가 연결이 되어 전원과 리셋 신호 및 클럭 신호가 입력되면, IC 카드는 필요한 정보의 신호를 단말기로 전송하게 되며, 이 전송된 신호를 수신한 마이크로콘트롤러에서는 필요한 프로토콜을 설정하게 된다.

이때, 본 발명의 IC카드 단말기는 단말기와 IC카드간에 필요한 정보 교환으로 카드내의 필요한 영역에 있는 데이터를 갱신할 수 있다. 또한 IC카드의 남은 금액이나 도수가 한계치에 도달할 때 이를 표시 장치를 통하여 사용자에게 알려주고, 필요시 수도·가스·전기 등의 계량기에 연결된 차단설비를 동작시켜 공급을 차단시키거나 자동차의 동작을 제어할 수 있다.

발명의 효과

이상에서 설명한 바와 같이, 본 발명의 다용도 접촉식 IC카드 단말기 및 그 제어방법에 의하면, 개인용 컴퓨터나 전화회선에 연결하지 않고도 독립적으로 전기·수도·가스·열량계 등의 각종 계량기나 자동차의 속도센서 및 엔진, 그리고 여러 가지 의료용 센서와 연결하여 사용량이나 자동차의 운행거리에 따라 요금이나 세금 등을 정산할 수 있고, 의료용의 각종 센서의 정보를 처리하여 기억할 수 있는 매우 뛰어난 효과가 있다.

아울러 본 발명의 바람직한 실시예들은 예시의 목적을 위해 개시된 것이며, 당업자라면 본 발명의 사상과 범위 안에서 다양한 수정, 변경, 부가등이 가능할 것이며, 이러한 수정 변경등은 이하의 특허청구범위에 속하는 것으로 보아야 할 것이다.

(57) 청구의 범위

청구항 1.

접촉식 IC카드 단말기 제어방법에 있어서,

상기 단말기와 IC카드의 접점이 연결되었는지 확인하는 과정과,

상기 IC카드의 접점 연결을 확인한 후, IC카드에 전원·리셋 신호·클럭 신호를 공급하고 통신용 단자를 단말기에 연결시키는 과정과,

상기 IC카드의 접점이 연결되지 않거나 통신 중 오류가 발생시 카드 인터페이스에서 공급하는 전원과 클럭 및 I/O를 차단시키고, 모든 동작을 처음으로 피드백시키는 과정과,

상기 리셋 신호를 공급받은 후 IC카드에서 보내는 신호를 수신하는 과정과,

상기 수신된 신호에 포함된 각 종 정보에 따라 단말기와 카드간에 전송시 필요한 프로토콜을 설정하는 과정과,

상기 단말기와 IC카드간에 응용에 필요한 정보를 교환하고 센서에서 입력된 아날로그나 디지털 신호들을 금액 또는 도수로 변환하여 카드내의 필요한 영역에 있는 데이터를 갱신하는 과정과,

상기 금액 또는 도수가 한계치에 도달할 때에는 표시장치를 통하여 사용자에게 알려주고 필요시 엔진이나 계량기에 연결된 차단설비를 동작시키는 신호를 출력하는 과정을 구비한 것을 특징으로 하는 접촉식 IC카드 단말기 제어방법.

청구항 2.
접촉식 IC카드 단말기에 있어서,

IC카드와 단말기를 연결하기 위한 콘넥터와, 상기 IC카드에 전원을 공급하는 전원회로부와, 상기 IC카드에 클럭/리셋 신호를 각각 발생시키는 클럭/리셋 신호발생회로부와, 마이크로콘트롤러의 출력단자에 연결하여 이들을 제어 할 수 있는 논리회로부로 구성된 IC카드 인터페이스 수단과,

자동차의 회전센서 또는 전기·수도·가스등의 계량장치나 의료용 센서에서 오는 아날로그 신호나 디지털 신호를 입력받아 단말기에 연결하여주는 회로로서, 각종 센서에서 유입되는 전압과 전류를 마이크로콘트롤러에 알맞는 전압과 전류로 정합하는 인터페이스 회로부를 포함하는 신호입력수단과,

상기 IC카드의 사용자·잔여금액·장치번호 등의 정보를 표시하며, 잔여금액이 일정치 이하로 내려갈 경우 이를 소리나 LED의 깜박임 또는 LCD의 숫자정보를 통하여 표시 및 경보하는 수단과,

상기 IC카드와 단말기에서 처리된 금액에 따라 해당된 전기·수도·가스등을 차단하거나 자동차의 동작을 제어하는 부분으로, 각 장치의 전기적 특성을 정합시키기 위한 인터페이스 회로부를 포함하는 출력 인터페이스 수단과,

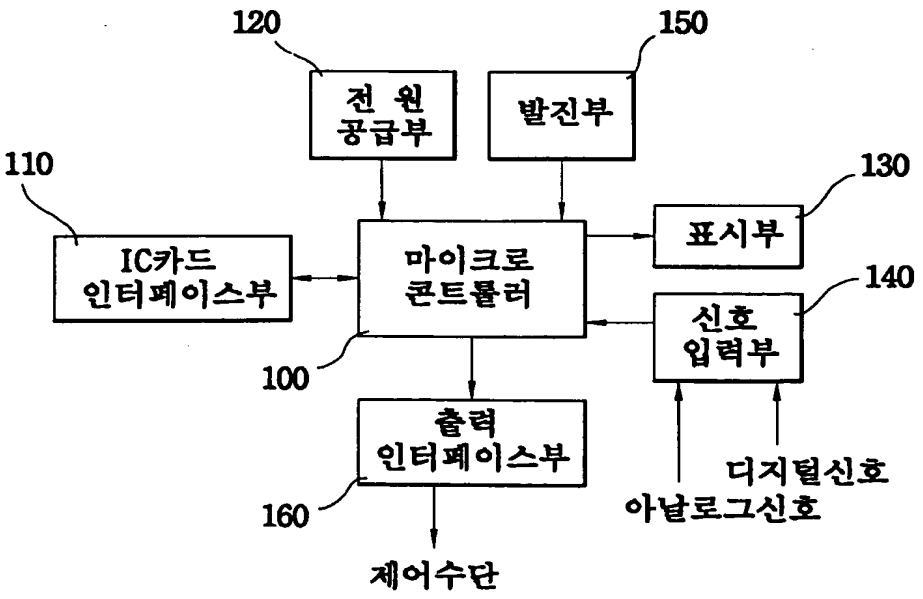
상기 IC카드 인터페이스 수단, 신호입력수단, 표시 수단, 출력 인터페이스 수단의 동작을 제어하는 마이크로콘트롤러와,

상기 마이크로콘트롤러를 동작시키기 위해서 필요한 클럭신호를 발생시키는 발진 수단과,

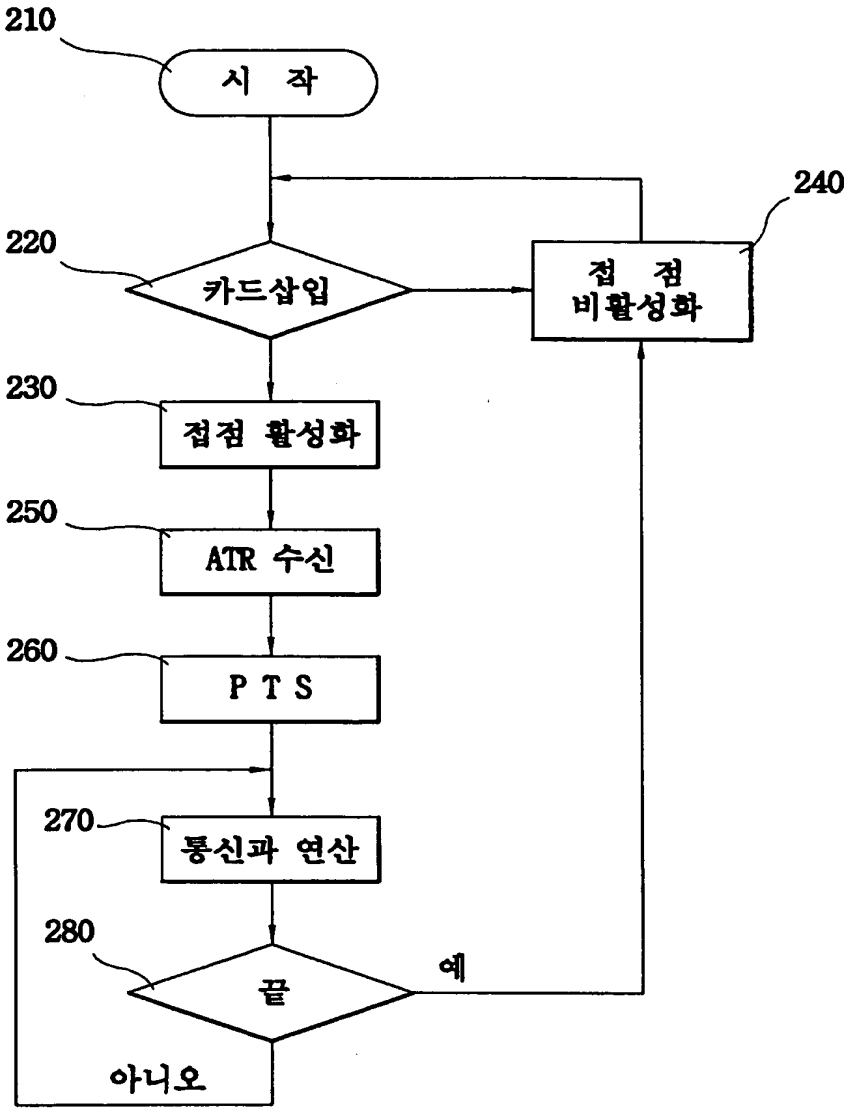
상기 마이크로콘트롤러나 IC카드 인터페이스 수단, 출력 인터페이스 수단, 표시 수단, 신호입력수단에서 사용할 직류전압을 공급하는 전원공급수단을 구비하여 이루어진 것을 특징으로 하는 다용도 접촉식 IC카드 단말기.

도면

도면 1



도면 2


210
시 작
240
220
카드삽입
접 점
비활성화
230
접점 활성화
250
ATR 수신
260
P T S
270
통신과 연산
280
끝
예
아니오

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.		(11) 공개번호	특2000-0006591
G06K 17/00		(43) 공개일자	2000년02월07일
(21) 출원번호	10-1998-0031419		
(22) 출원일자	1998년08월01일		

(71) 출원인	이종인 대한민국 139-223 서울특별시 노원구 중계3동 511-2호 중계 제1공단 601호 김강형 대한민국 158-070 서울특별시 양천구 신정동 325번지 목동 신시가지아파트 1109동 1007호
(72) 발명자	이종인 대한민국 156-020 서울특별시 동작구 대방동 23-15 대방2단지 주공아파트 210-1203호 김강형 대한민국 158-070 서울특별시 양천구 신정동 325번지 목동 신시가지아파트 1109동 1007호
(74) 대리인	문경진 조현석
(77) 심사청구	있음

(54) 출원명 IC카드 다중-엑세스 시스템 및 방법

요약

본 발명은 하나의 IC 카드 엑세스수단을 이용하여 다수개의 IC 카드를 엑세스할 수 있는 IC 카드 다중-엑세스 시스템 및 방법에 관한 것으로서, IC 카드 리셋과 동시에 해당 카드로부터 출력되는 리셋 기본정보(ATR)의 패턴을 검출하여 자신이 기억하고 있는 ATR 패턴중의 하나인 경우 해당 패턴을 갖는 카드 발급사의 엑세스 명령군을 자동으로 선택하여 해당 엑세스 명령군에 따라 IC 카드를 읽거나 쓰는 IC 카드 엑세스 시스템; 및 IC 카드가 투입되는 초기에 카드를 리셋시킴과 동시에 해당 카드로부터 출력되는 리셋 기본정보(ATR)의 패턴을 검출하는 제 1단계; 상기 검출된 ATR 패턴이 미리 저장된 다수의 ATR 패턴중의 하나와 일치되는지를 탐색하는 제 2단계; 상기 탐색결과 ATR 패턴이 일치되는 카드 발급사의 엑세스 명령군을 선택하여 해당 엑세스 명령군에 따라 IC 카드를 읽거나 쓰는 제 3단계의 처리단계로 이루어진 것을 특징으로 한다.

대표도

도3

명세서

도면의 간단한 설명

도 1은 종래의 IC카드 엑세스 시스템의 블록도

도 2는 본 발명의 일 실시예에 따른 IC 카드 다중-엑세스 시스템의 블록도

도 3은 본 발명의 일 실시예에 따른 IC카드 다중-엑세스 시스템의 또 다른 블록도

도 4는 본 발명의 다른 실시예에 따른 IC 카드 다중-엑세스 방법을 설명하기 위한 동작 흐름도

도 5는 도 4의 제 3단계 처리과정을 상세하게 도시한 동작 흐름도

** 도면의 주요 부분에 대한 부호의 설명**

100 : IC카드 다중-엑세스 제어수단 1101-110n : IC 보안모듈(SAM)

120 : IC카드 판독/기록부 1301-130n : IC 카드

140 : 메모리수단

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 반도체 칩(IC)을 정보기록매체로 사용하여 반도체 칩과의 접촉 또는 비접촉 방식에 의해 카드정보를 읽거나 쓸수 있는 IC카드 엑세스 시스템에 관한 것으로서, 특히 IC카드가 투입되는 초기에 카드에 전원을 공급하여 카드를 리셋시킬때에 그와 동시에 카드에서 발생되는 리셋기본정보(Answer To Reset: 이하 ATR이라 약칭함)의 패턴(pattern) 비교에 의하여 IC 카드에 맞는 엑세스 명령군을 자동으로 선택하여 카드를 엑세스할 수 있도록 함으로써, 각각 발급사가 다른 여러 종류의 IC 카드를 하나의 엑세스 시스템에서 읽거나 쓸 수 있도록 하는 IC카드 다중-엑세스시스템 및 방법에 관한 것이다.

종래의 IC 카드 엑세스 시스템은 도 1에 도시된 바와 같이 지정된 하나의 IC 카드(13)를 엑세스하기 위한 IC 카드 판독/기록부(12)와, 상기 IC카드 판독/기록부에서 독출된 카드정보를 이용하여 카드의 코드번호 체계와 식별번호를 추출하여 카드의 정당성을 검증하고, 그 검증결과 자신에 해당하는 정당한 정보일 경우 그에 따른 부가정보를 생성하여 상기 IC 카드 판독/기록부로 전송하는 IC 보안모듈(SAM; 11)로 구성된다.

상기와 같이 자신만의 IC 보안모듈(11, 21)을 각각 개별적으로 구비한 하나의 카드 판독/기록부(12, 22)가 한 종류의 IC 카드(13, 23)만을 읽고 쓰기 때문에 각각 발급사가 다른 여러 종류의 IC카드를 읽고 쓰기 위해서는 엑세스하고자 하는 IC 카드 개수만큼 상기 IC카드 판독/기록부(12, 22)와 IC 보안모듈(11, 21)을 각각 설치하여야만 카드 발급사가 서로 다른 여러 종류의 IC 카드를 읽고 쓸 수 있게 된다.

그러나 상기와 같이 엑세스 시스템을 구성할 경우 매 카드마다 해당 발급사의 IC카드 판독/기록부와 IC 보안모듈이 각각 구비되어야 하므로 IC 카드 엑세스 시스템이 매우 복잡하게 구성되고, 제작단가가 증가되어 원가 절감을 위한 개선책이 요구되는 등의 문제점이 있었다.

발명이 이루고자 하는 기술적 과제

따라서 본 발명은 상기의 필요성에 부응할 수 있으면서 기존의 문제점을 해결하기 위해 창출한 것으로서, 본 발명은 IC 카드로부터 출력되는 리셋기본정보(ATR)의 패턴 비교에 의해 IC 카드에 맞는 엑세스 명령군을 자동으로 선택하여 해당 엑세스 명령군에 따라 IC 카드를 읽거나 쓰도록 제어함으로써, 하나의 IC 카드 엑세스 시스템을 사용하여 엑세스 명령군이 서로 다른 여러종류의 IC 카드를 읽고 쓸수 있는 IC 카드 다중-엑세스 시스템 및 방법을 제공함에 그 목적이 있다.

상기의 목적을 달성하기 위하여 본 발명의 일 실시예에서는 IC 카드에 정보를 쓰거나 읽는 IC 카드 판독/기록부와; 상기 IC 카드 판독/기록부에서 IC 카드가 감지되면 IC 카드 리셋과 동시에 IC 카드로부터 출력되는 리셋기본정보(ATR)의 패턴을 검출하고, 검출된 패턴을 이용하여 해당 IC 카드에 맞는 엑세스 명령군을 자동으로 탐색하여 해당 엑세스 명령군에 따라 IC 카드를 엑세스하도록 상기 IC카드 판독/기록부를 제어하는 IC 카드 다중-엑세스 제어수단; 상기 IC카드 판독/기록부에서 독출된 정보를 상기 제어수단으로부터 제공받아 카드의 코드번호 체계와 식별번호를 추출하여 카드의 정당성을 검증하고, 그 검증결과에 따른 부가정보를 생성하여 다시 제어수단으로 제공하는 IC 보안모듈(SAM)과; 다수의 IC 카드 종류별 ATR 패턴과 해당 엑세스 명령군을 저장하는 메모리수단을 구비한 IC 카드 다중-엑세스 시스템을 제공한다.

상기의 목적을 달성하기 위하여 본 발명의 다른 실시예에서는 IC 카드 리셋과 동시에 해당 카드로부터 출력되는 리셋 기본정보(ATR)의 패턴을 검출하는 제 1단계; 미리 저장된 다수의 ATR 패턴과 상기 검출된 ATR 패턴을 비교하여 현재 판독된 IC 카드의 발급사를 탐색하는 제 2단계; 상기 해당 카드 발급사의 엑세스 명령군을 선택하여 해당 엑세스 명령군에 따라 IC 카드 엑세스를 실행하는 제 3단계의 처리과정을 갖는 IC 카드 다중-엑세스 제어방법을 제공한다.

발명의 구성 및 작용

이하, 본 발명에 따른 IC 카드 다중-엑세스 시스템 및 방법과 그 작용 효과를 첨부된 도면에 의거하여 상세히 설명한다.

도 2와 도 3은 본 발명의 일 실시예에 따른 IC 카드 다중-엑세스 시스템의 블록도로서, IC 카드 판독/기록부(120)는 IC 카드에 전원과 클럭신호를 공급하여 카드를 리셋시킨 후 제어수단에서 주어지는 엑세스 명령에 따라 IC 카드에 정보를 쓰거나 IC카드로부터 정보를 읽거나 쓸 수 있으며, 이를 위하여 상기 IC카드 판독/기록부(120)는 IC 카드를 투입할 수 있는 카드 투입구가 마련되고, 상기 카드 투입구 내부에 카드가 투입구에 투입될 때 카드정보를 인식한다.

다수개의 IC 카드(1301-130n)들은 상기 IC카드 판독/기록부(120)에서 전원과 클럭신호가 공급되어 리셋동작이 실행되면 그와 동시에 IC카드 자체에 대한 기본 정보(ATR)를 자동으로 출력하게 된다.

한 개의 IC 보안모듈(SAM; 110) 또는 다수개의 IC 보안모듈(1101-110n)은 각각의 IC카드(1301-130n) 발급사가 제공하는 보안장치로서, 상기 IC카드 판독/기록부에서 독출된 카드정보로부터 카드의 코드번호 체계와 식별번호를 추출하여 카드의 정당성을 검증하고, 그 검증결과 자신에 해당하는 정당한 정보일 경우 그에 따른 부가정보 즉, 상기 IC 카드 판독/기록부의 카드 엑세스 동작을 제어하기 위한 명령이나 쓰기 데이터 등의 정보를 각각 생성한다. 또한 상기 IC 보안모듈(110, 1101-110n)은 상기 IC 카드 판독/기록부에 대하여 단독으로 혹은 각각 병렬로 연결되며, 판독된 카드정보 중의 일부 예컨대, 비밀키, 공개키와 같은 소정의 암호화 방식에 의해 암호화시켜 보안성을 확보할 수도 있다.

메모리수단(140)은 카드 발급사가 다른 다수 IC 카드종류별 ATR 패턴과 엑세스 명령군을 기억시키기 위한 메모리로서, 저장되는 데이터는 예를 들어 아래의 표 1과 같은 방식으로 저장할 수 있다.

[표 1]

분류번호(N)	카드종류	ATR 패턴	엑세스명령군
1	MP COS	0x3B,0x24,0x00m0x80,0x72,0xA4,0x45	GEM plus COS
2	삼성 SCOS	0x3B,0x6F,0x00,0x00,0x01,0x05,0x0A,0x00,0x00,0x00,0x00,0x00, 0x00,0x00,0x00,0x00	삼성 SCOS
3	Multiflex3KG2	0x3B,0x02,0x14,0x50	Schlumberger
4	Multiflex8KG2	0x3B,0x32,0x15,0x00,0x06,0x80	Schlumberger
5	Siemens COS	0x3B,0xB7,0x11,0x00,0x81,0x31,0x90,0x73,0x22,0x04,0xAB,0xC8,0x03,0x1C,0x09,0xA6	Siemens COS
6	Hitachi COS	0x3B,0xF0,0x11,0x00,0x00,0x70,0x64,0x00,0x01,0xED	Hitachi COS

7	LG COS2..0	0x3B,0x60,[redacted]0,0x00,0x80,0x31, 0x90,0x63,0x4C,0x47,0x20,0x71,0xB7,0x83,0x0B,0xFF,0x10, 0x11,0xFE	LG COS

IC 카드 다중-엑세스 제어수단(100)은 상기 IC카드 판독/기록부(120)의 카드 초기화동작 및 엑세스동작을 제어할 수 있는 마이크로 컴퓨터로서, IC카드에서 출력되는 리셋 기본정보(ATR)의 패턴을 상기 IC 카드 판독/기록부를 통해 검출하고, 그것과 상기 메모리 수단에 기억시킨 각 카드 종류별 패턴과의 비교에 의해 해당 카드 발급사의 엑세스 명령군을 선택하여 해당 엑세스 명령군에 따라 IC 카드를 읽거나 쓰도록 IC 카드 엑세스 동작을 제어한다.

이때 상기 표 1에서 알 수 있는 바와 같이 카드 발급사가 동일한 직불 또는 선불 또는 신용 IC 카드에 대해서는 동일한 엑세스 명령군에 의해 엑세스동작을 제어할 수 있으므로 카드 발급사를 탐색하는 동작으로도 충분히 IC 카드 엑세스 명령군을 탐색할 수 있게 된다.

여기서 상기 요소들 즉, IC 카드 판독/기록부와; 이것에 단독으로 혹은 각각 병렬로 연결된 한 개 혹은 다수개의 IC 보안모듈(SAM)과; 상기 IC카드 엑세스수단과 IC 보안모듈 사이에서 상기 IC카드의 엑세스동작을 제어하는 IC카드 다중-엑세스 제어수단; IC 카드종류별 ATR 패턴과 엑세스 명령군을 저장하는 메모리수단을 하나의 기판위에 실장하고, 그 전체를 한몸으로 봉합하여 하이브리화시킴으로써, 엑세스 명령군이 다른 여러 종류의 IC 카드를 엑세스할 수 있는 집적회로를 구현할 수 있다.

또한 상기 IC 카드 판독/기록부와; 상기 IC 카드 다중-엑세스 제어수단과; 상기 메모리수단을 하나의 기판위에서 한몸으로 원칩화시켜 다기능 원칩으로 구현할 수 있다.

도 4는 본 발명의 다른 실시예에 따른 IC 카드 다중-엑세스 방법을 설명하기 위한 동작 흐름도로서, 상기 IC 카드 다중-엑세스 제어수단(100)이 다수개의 IC카드 엑세스를 위하여 실행하는 동작 과정을 예를 들어 도시하고 있으며, 이러한 동작과정은 본 발명의 IC 카드 다중-엑세스 시스템에서도 동일한 과정으로 엑세스동작이 실행될 수 있다.

상기 동작 흐름도에서 제 1단계는 IC 카드가 투입된 것이 판단되면 IC 카드 판독/기록부(120)로 리셋 명령을 내려 IC 카드에 전원과 클럭신호를 공급하여 카드를 리셋시키는 단계(S101, S102)와, 상기 IC 카드 리셋동작이 실행될때에 해당 카드로부터 출력되는 IC카드의 리셋 기본정보(ATR) 패턴(ATR 패턴(0))을 검출하는 단계(S103)로 이루어지며, 이 단계에서 현재 IC 카드 판독/기록부에 투입된 카드의 ATR 패턴을 검출한다.

제 2단계는 분류번호(N)를 초기치 "1"로 설정하여 상기 표 1의 첫 번째 ATR패턴(1)을 읽어들이는 단계(S104, S105)와, 첫 번째 ATR 패턴(1)을 상기 검출된 ATR 패턴(0)과 비교하는 단계(S106)와, 상기 비교결과 두 패턴이 일치하지 않으면 분류번호를 "1"씩 증가시키는 단계(S107, S108)로 이루어지며, 여기서 증가된 값을 이용하여 다시 상기 표 1의 ATR 패턴을 순차적으로 읽어들여 다시 비교하는 단계(S105, 106)로 복귀하게 된다. 이 단계에서는 IC 카드에서 검출된 ATR 패턴(0)과 일치하는 ATR 패턴을 탐색함으로써, 현재 투입된 IC카드가 엑세스 가능한 카드인지를 판단한다.

제 3단계는 상기 탐색결과 엑세스 가능한 카드인 경우 ATR 패턴이 일치되는 카드 발급사의 엑세스 명령군을 선택하는 단계(S109)와, 상기 선택된 해당 엑세스 명령군에 따라 IC 카드를 읽거나 쓰는 엑세스를 실행하는 단계(S110)로 이루어지며, 여기서는 엑세스 가능한 카드인 경우 ATR 패턴이 일치되는 카드 발급사의 엑세스 명령군에 따라 IC 카드를 읽거나 쓰는 엑세스를 실행하고, 엑세스 불가능한 카드일 경우는 프로세스 에러메시지를 표시(S111)한다.

도 5는 상기 도 4의 엑세스 실행 과정(S110)을 상세하게 설명하기 위한 동작 흐름도로서, 제 31단계(S311-S313)에서는 IC카드 판독/기록부에서 카드가 감지되면 우선 그 카드의 공통 메모리영역을 엑세스하는 공통 메모리 엑세스과정을 수행한다.

제 32단계(S314-315, S326-327, S330-331)에서는 상기 공통 메모리영역에서 엑세스된 정보를 미리 정해진 정보전송방법에 따라 다수개의 IC 보안모듈(SAM)로 전송하는 공통정보 송신과정을 수행한다. 이때 상기 IC카드 다중-엑세스 제어수단에서는 다수개의 IC 보안모듈의 주소를 각각 구별하지 않은 상태에서 일제히 전체 IC 보안모듈로 엑세스 정보를 전송하는 과정을 실행할 수 있으며, 또한 다수개의 IC 보안모듈의 주소를 각각 구별한 상태에서 그 주소를 하나씩 증가시키면서 각각 개별적으로 해당 주소의 IC 보안모듈에 엑세스 정보를 전송하는 과정을 실행할 수 있다.

제 33단계(S316, S328)에서는 상기 다수개의 IC 보안모듈중 어느 하나로부터 생성된 코드번호체계 검증결과와 카드 고유의 식별번호 검증결과 및 메모리 엑세스(읽기나 쓰기)를 위한 데이터와 명령정보를 수신하는 검색정보 수신과정을 수행한다. 여기서 메모리 엑세스를 위한 데이터 및 명령정보는 해당 SAM의 주소, IC 카드의 고유 메모리영역정보, IC카드를 읽거나 쓰기 위한 메모리 엑세스 방법, 쓰기 위한 데이터, 사용될 키 값 등을 들수 있다.

제 34단계(S317-S323, S329)에서는 상기 수신된 데이터와 명령정보를 이용하여 상기 IC카드의 고유 메모리영역을 엑세스하고, 그 메모리 엑세스 결과를 해당 IC 보안모듈로 다시 전송하는 고유메모리 엑세스 및 전송과정이다. 즉 이때에는 읽기 요청인 경우 IC카드의 해당 메모리영역을 키를 이용하여 읽어 해당 SAM으로 전송하는 과정이 실행될 수 있으며, 쓰기 요청인 경우 IC카드의 해당 메모리 영역에 키를 이용하여 수신 데이터를 쓰는 과정이 실행될 수 있다.

제 35단계(S324-325, S332)에서는 상기 재전송 후 해당 IC 보안모듈로부터 추가명령이 수신되는지를 판단하고, 추가명령이 수신되면, 수신정보에 따라 추가명령을 실행하기 위해 상기 제 34단계로 복귀하고, 그 외의 경우 현재 검증된 IC 카드에 대한 모든 엑세스 동작을 종료하게 된다.

이때에도 상기 각 처리단계에서 에러가 발생하는 경우는 그 상태를 표시하는 단계를 더 포함할 수 있고, 이후에는 현재 독출된 IC카드에 대한 모든 메모리 엑세스 동작을 종료하게 된다.

이상에서와 같은 본 발명의 시스템 및 방법은 이미 서술된 시스템뿐만 아니라 그밖에도 단말기와 여러 유사한 장비 또는 반도체 칩 등에 쉽게 적용가능함은 물론이다.

발명의 효과

이상에서와 같은 본 발명에 의하면 리셋전원과 클럭신호에 의해 IC 카드가 리셋될때에 해당 카드로부터 자동 출력되는 리셋 기본정보(ATR)의 패턴을 검사하는 동작으로 하나의 IC 카드 엑세스 시스템에서 다수개의 IC 카드를 수용할 수 있게 되므로 IC 카드 엑세스 시스템을 작은 부피로 간단하게 구성할 수 있으며, 따라서 제작단가를 줄여 원가 절감 효과를 얻을 수 있으며, 또한 각각의 카드 제작사가 다르기 때문에 발생되는 IC카드들의 비호환성 문제를 하나의 카드 단말기를 사용하여 해결할 수 있는 이점이 있게 된다.

(57) 청구의 범위

청구항 1.

IC 카드에 정보를 쓰거나 읽는 IC 카드 판독/기록부와; 상기 IC 카드 판독/기록부에서 IC 카드가 감지되면 IC 카드 리셋과 동시에 IC 카드로부터 출력되는 리셋기본정보(ATR)의 패턴을 검출하고, 검출된 패턴을 이용하여 해당 IC 카드에 맞는 엑세스 명령군을 자동으로 탐색하여 해당 엑세스 명령군에 따라 IC 카드를 엑세스하도록 상기 IC카드 판독/기록부를 제어하는 IC 카드 다중-엑세스 제어수단; 상기 IC카드 판독/기록부에서 독출된 정보를 상기 제어수단으로부터 제공받아 카드의 코드번호 체계와 식별번호를 추출하여 카드의 정당성을 검증하고, 그 검증결과에 따른 부가정보를 생성하여 다시 제어수단으로 제공하는 IC 보안모듈(SAM)과; 다수의 IC 카드 종류별 ATR 패턴과 해당 엑세스 명령군을 저장하는 메모리수단을 구비한 IC 카드 다중-엑세스 시스템.

청구항 2.

제 1항에 있어서, 상기 IC 보안모듈이 상기 제어수단에 대하여 다수개가 병렬로 연결되어 상기 제어수단으로부터 전송되는 정보를 이용하여 카드의 코드번호 체계와 식별번호를 검증하고, 그 검증결과 자신에 해당하는 정당한 정보일 경우 그에 따른 부가정보를 생성하여 자신의 주소와 함께 상기 제어수단으로 제공하는 것을 특징으로 하는 IC 카드 다중-엑세스 시스템.

청구항 3.

제 2항에 있어서, 상기 IC카드 다중-엑세스 제어수단은 상기 IC카드에서 엑세스된 정보를 다수개의 IC 보안모듈 전체에 동시에 전송하는 것을 특징으로 하는 IC카드 다중-엑세스 시스템.

청구항 4.

제 2에 있어서, 상기 IC카드 다중-엑세스 제어수단은 상기 IC카드에서 엑세스된 정보에 다수개의 IC 보안모듈의 각 주소를 부여하여 개별적으로 전송하는 것을 특징으로 하는 IC카드 다중-엑세스 시스템.

청구항 5.

제 1항에 있어서, 상기 IC 카드 판독/기록부와; 상기 다수개의 IC 보안모듈과; 상기 IC 카드 다중-엑세스 제어수단과; 상기 메모리수단을 하나의 기판위에 실장하고, 그 전체를 한몸으로 봉합하여 하이브리드칩화시킨 것을 특징으로 하는 무선 정보기록매체 다중-엑세스 시스템.

청구항 6.

제 1항에 있어서, 상기 IC 카드 판독/기록부와; 상기 IC 카드 다중-엑세스 제어수단과; 상기 메모리수단을 하나의 기판위에서 한몸으로 원칩화시킨 것을 특징으로 하는 무선 정보기록매체 다중-엑세스 시스템.

청구항 7.

IC 카드 리셋과 동시에 해당 카드로부터 출력되는 리셋 기본정보(ATR)의 패턴을 검출하는 제 1단계; 미리 저장된 다수의 ATR 패턴과 상기 검출된 ATR 패턴을 비교하여 현재 판독된 IC 카드의 발급사를 탐색하는 제 2단계; 상기 해당 카드 발급사의 엑세스 명령군을 선택하여 해당 엑세스 명령군에 따라 IC 카드 엑세스를 실행하는 제 3단계를 구비한 IC 카드 다중-엑세스 방법.

청구항 8.

제 6항에 있어서, 상기 제 3단계는 IC 카드의 공통 메모리영역을 엑세스하는 제 31단계; 상기 공통 메모리영역에서 엑세스된 정보를 미리 정해진 정보전송방법에 따라 다수개의 IC 보안모듈로 전송하는 제 32단계; 상기 다수개의 IC 보안모듈중 어느 하나로부터 생성된 코드번호체계 검증결과와 식별번호 검증결과 및 메모리 엑세스(읽기나 쓰기)를 위한 데이터와 명령정보를 수신하는 제 33단계; 상기 수신된 데이터와 명령정보를 이용하여 상기 IC카드의 고유 메모리영역을 엑세스하고, 그 메모리 엑세스 결과를 해당 IC 보안모듈로 다시 전송하는 제 34단계; 상기 재전송 후 해당 IC 보안모듈로부터 추가명령이 수신되면 수신정보에 따른 명령을 실행하기 위해 상기 제 34단계로 복귀하고, 그 외의 경우 현재 검증된 IC카드 엑세스에 대한 모든 동작을 종료하는 제 35단계의 처리단계를 구비하여 하나의 IC카드 판독/기록수단을 이용하여 다수개의 IC카드를 엑세스할 수 있게 한 IC 카드 다중-엑세스 방법.

청구항 9.

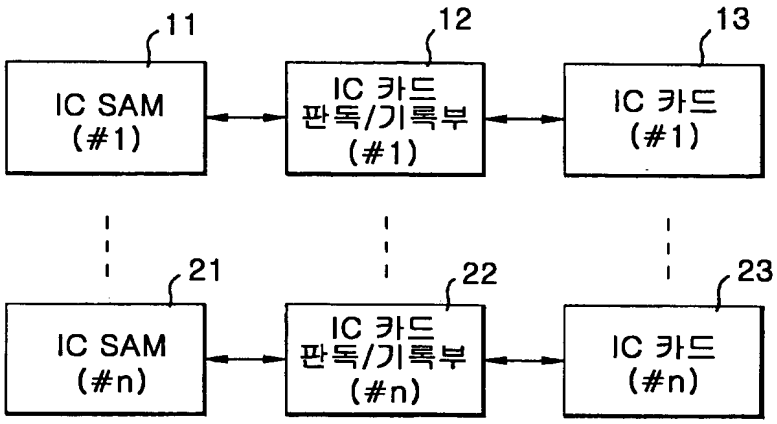
제 7항에 있어서, 상기 제 32단계는 다수개의 IC 보안모듈의 주소를 각각 구별하지 않은 상태에서 일제히 전체 IC 보안모듈로 엑세스 정보를 전송하는 것을 특징으로 하는 IC카드 다중-엑세스 방법.

청구항 10.

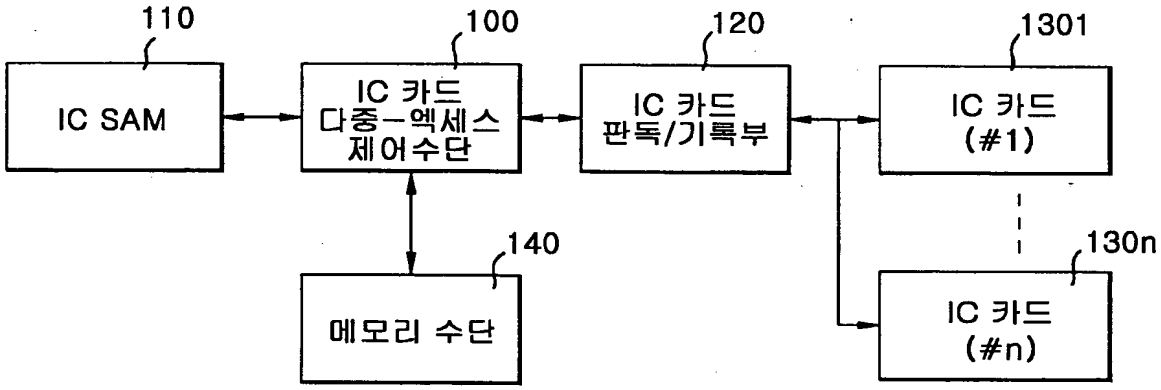
제 7항에 있어서, 상기 제 32단계는 다수개의 IC 보안모듈의 주소를 각각 구별한 상태에서 그 주소를 하나씩 증가시키면서 각각 개별적으로 엑세스 정보를 전송하는 것을 특징으로 하는 IC카드 다중-엑세스 방법.

도면

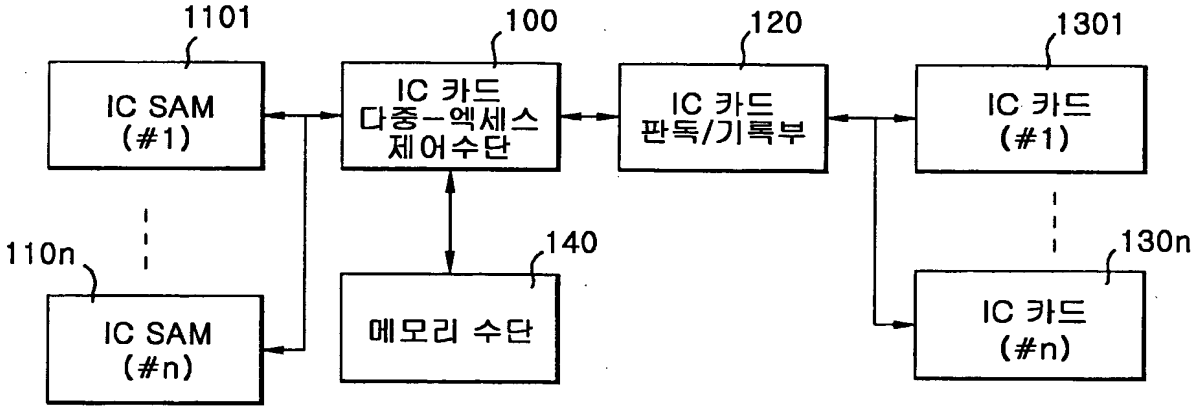
도면 1


11
12
13
IC SAM
(#1)
IC 카드
판독/기록부
(#1)
IC 카드
(#1)
21
22
23
IC SAM
(#n)
IC 카드
판독/기록부
(#n)
IC 카드
(#n)

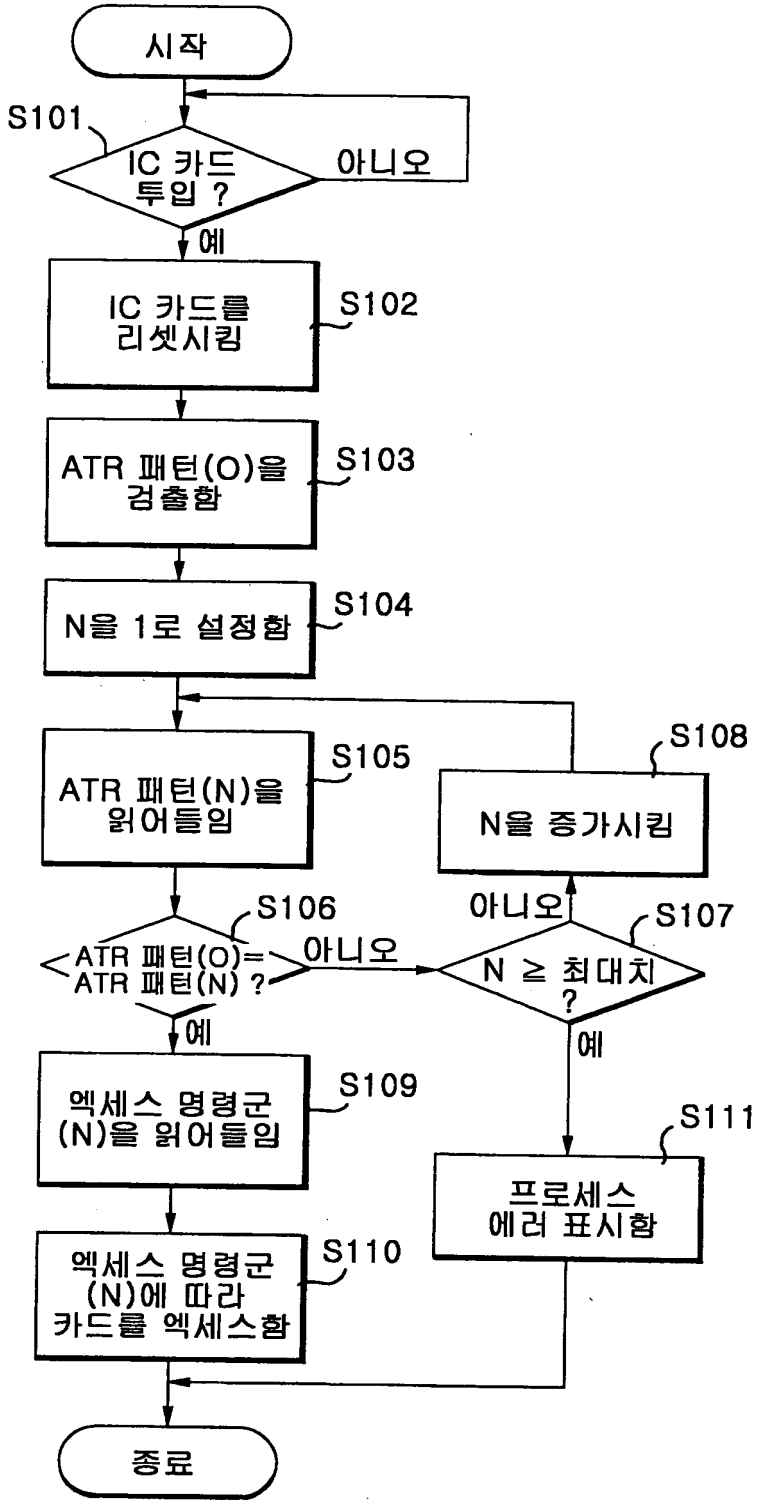
도면 2


110
100
120
1301
IC SAM
IC 카드
다중-엑세스
제어수단
IC 카드
판독/기록부
IC 카드
(#1)
140
130n
메모리 수단
IC 카드
(#n)

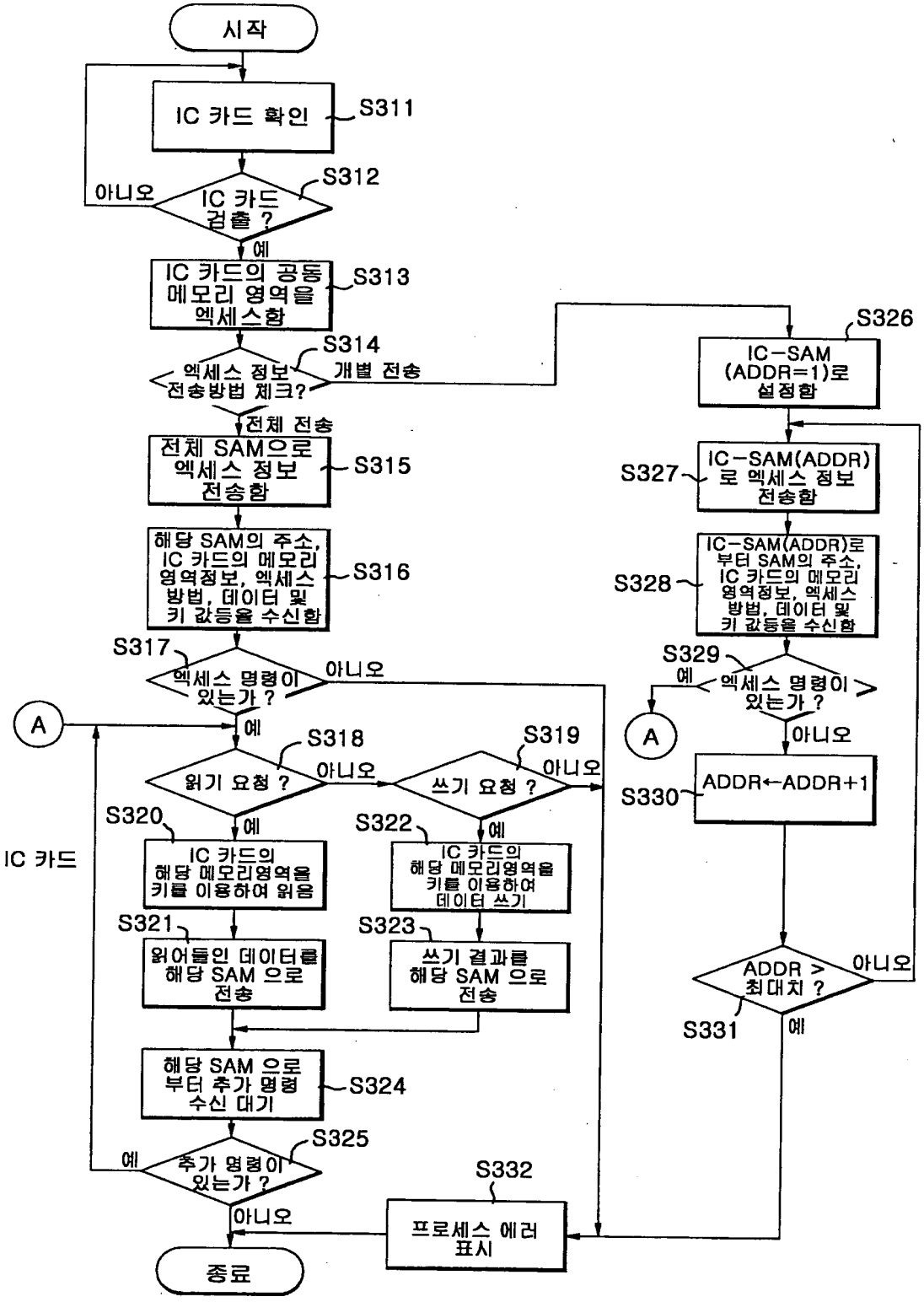
도면 3


1101
100
120
1301
IC SAM
(#1)
IC 카드
다중-엑세스
제어수단
IC 카드
판독/기록부
IC 카드
(#1)
110n
140
130n
IC SAM
(#n)
메모리 수단
IC 카드
(#n)

도면 4


시작
S101
IC 카드 투입 ?
아니오
예
IC 카드를 리셋시킴
S102
ATR 패턴(O)을 검출함
S103
N을 1로 설정함
S104
ATR 패턴(N)을 읽어들임
S105
S108
N을 증가시킴
S106
ATR 패턴(O)= ATR 패턴(N) ?
아니오
아니오
S107
N ≥ 최대치 ?
예
예
엑세스 명령군 (N)을 읽어들임
S109
S111
프로세스 에러 표시함
엑세스 명령군 (N)에 따라 카드를 엑세스함
S110
종료

도면 5


시작
IC 카드 확인
S311
IC 카드 검출 ?
S312
아니오
예
IC 카드의 공동 메모리 영역을 엑세스함
S313
엑세스 정보 전송방법 체크?
S314
개별 전송
전체 전송
전체 SAM으로 엑세스 정보 전송함
S315
해당 SAM의 주소, IC 카드의 메모리 영역정보, 엑세스 방법, 데이터 및 키 값등을 수신함
S316
엑세스 명령이 있는가 ?
S317
아니오
예
A
읽기 요청 ?
S318
아니오
쓰기 요청 ?
S319
아니오
예
IC 카드
IC 카드의 해당 메모리영역을 키를 이용하여 읽음
S320
읽어들인 데이터를 해당 SAM 으로 전송
S321
IC 카드의 해당 메모리영역을 키를 이용하여 데이터 쓰기
S322
쓰기 결과를 해당 SAM 으로 전송
S323
해당 SAM 으로부터 추가 명령 수신 대기
S324
추가 명령이 있는가 ?
S325
예
아니오
종료
IC-SAM (ADDR=1)로 설정함
S326
IC-SAM(ADDR) 로 엑세스 정보 전송함
S327
IC-SAM(ADDR)로부터 SAM의 주소, IC 카드의 메모리 영역정보, 엑세스 방법, 데이터 및 키 값등을 수신함
S328
엑세스 명령이 있는가 ?
S329
예
아니오
A
ADDR←ADDR+1
S330
ADDR > 최대치 ?
S331
아니오
예
프로세스 에러 표시
S332

PKCS #15 기반의 무선인증모듈 설계 및 구현

강유성*

*한국전자통신연구원, 무선인터넷정보보호연구팀

Design and Implementation of WIM based in PKCS #15

You Sung Kang*

*Wireless Internet Security Research Team, ETRI.

요 약

무선인터넷 접속 프로토콜의 사실상 국제표준이라 할 수 있는 WAP 프로토콜의 규격을 제정하는 WAP 포럼에서는 인증서 및 비밀키의 저장, 그리고 암/복호화 및 전자서명/검증 등의 연산을 지원하기 위한 무선인증모듈 규격을 정의하고 있다. 스마트카드로 구현되는 무선인증모듈의 사용 형태를 고려할 때, 다양한 플랫폼에서의 사용과 사용자의 이동성 지원, 그리고 무선인증모듈을 이용한 정보보호 특성 보장은 필수적인 요구조건이다. 본 논문은 무선인증모듈을 스마트카드로 구현함에 있어 멀티 애플리케이션을 지원하고, 기능 확장성을 보장하기 위한 PKCS #15 기반의 무선인증모듈 설계와 구현 결과를 보인다. 본 논문에서는 접촉형 스마트카드에 대한 국제규격인 ISO/IEC 7816 시리즈 규격을 준수한 설계를 보이고, 지수승 모듈러 연산을 하드웨어적으로 지원받아 RSA 1024 비트 암/복호화 및 전자서명/검증을 처리하는 결과를 보인다.

I. 서론

WAP (Wireless Application Protocol) 포럼에서 연구중인 WAP 프로토콜과 마이크로소프트사의 ME (Mobile Explorer) 솔루션은 무선인터넷 사용의 활성화에 기여했던 대표적인 무선인터넷 접속 규격이다. 무선인터넷을 이용하는 안전한 사이버 공간을 구축하기 위해서는 기밀성(Privacy), 무결성(Integrity), 인증(Authentication), 부인방지(Non-repudiation), 접근제어(Access control) 및 신원확인(Authorization) 등 전송 정보의 정보보호 특성을 만족시키기 위한 기술개발이 병행되어야 한다.

WAP 프로토콜을 살펴볼 때, 정보보호와 관련된 요소는 WTLS (Wireless Transport Layer Security), WMLScript Crypto Library, WPKI (Wireless Public Key Infrastructure), 그리고 WIM (WAP Identity Module) 등이다. WTLS는 유선에서 사용하는 전송계층 보안 프로토콜인 SSL (Secure Socket Layer)/ TLS (Transport Layer Security)와 유사한 구조를 가지면서 무선환경에 적합하도록 구성된 프로토콜로써 무선전송계층에서 클라이언트와 서버 사이의 인증 및 세션 키 분배를 담당한다. WMLScript Crypto Library 규격에서는 전자서명을 위한 함수를 제공하고 있으며, WPKI는 공개키 기반 구조를 무선환경으로 확장한 형태로써 WTLS와 WMLScript Crypto Library 규격이 기본적으로 공개키 인증서에 기반하고 있다. WIM은 WTLS 계층에서의 데이터 암/복호화와 전자서명/검증을 지원하고 응용 계층에서의 전자서명, 암호화 키의 복호화 동작을 지원한다. 특히 WIM은 정보보호 측면에서 볼 때 비밀키와 공인 인증기관 인증서의 안전한 저장을 보장하는 장점을 지니고 있으며, 그 구현형태는 스마트카드 형태를 띠기 때문에 향후 멀티 애플리케이션 카드에 하나의 응용으로 사용되어 스마트카드 사용자에게 안전한 정보보호 서비스 제공에 기여할 수 있다.

본 논문에서는 WAP 프로토콜의 정보보호 관련 요소 중 무선인증모듈에 해당하는 WIM 내부 구조의 소프트웨어 설계에 있어 멀티 애플리케이션을 지원하며 기능 확장성이 보장되는 PKCS #15 (Public-Key Cryptography Standards #15) 기반의 효율적인 계층화 구조 설계를 제시하고 그 구현 결과에 관하여 상세히 기술한다. 본 논문의 구성은 다음과 같다. II장에서 WIM을 스마트카드 형태로 구현하기 위한 국제규격 및 관련 기술을 분석한다. 분석된 국제규격 및 관련 기술을 기반으로 WIM 모듈을 설계한 내용을 III장에서 설명하고, IV장에서는 설계된 WIM 모듈의 구현 결과 및 WIM 기능 처리 능력을 분석한다. 끝으로 V장에서 결론을 맺는다.

II. 스마트카드 구현 기술

1. WIM

보안기능을 강화하기 위하여 보안기능 처리를 위한 별도의 불법변조 방지장치(tamper-resistant device)를 사용할 수 있다. 이러한 불법변조 방지장치는 불법적인 공격자로부터 사용자의 중요 데이터를 보호하는 역할을 한다. WAP 프로토콜의 정보보

호 관련 요소 중 이러한 불법변조 방지장치 역할을 하는 요소가 WIM (WAP Identity Module)이다. WIM은 비밀키와 인증기관 인증서와 같은 중요 정보를 저장하고 있으며, 이러한 중요 정보를 이용한 암호연산을 수행하고, master secret을 계산하고 저장하는 동작을 수행한다.

WIM은 무선단말기의 보안 취약성을 보완하는 보안토큰(crypto token)으로써 기능적인 측면에서 볼 때, WTLS 계층에서의 암호연산을 지원하고, 응용계층에서의 전자서명을 지원한다[1]. 그림 1은 WIM을 포함하는 WAP 프로토콜의 아키텍처를 나타내고 있다. 그림 1에서 보이는 것처럼 WIM은 어느 특정계층만을 지원하는 것이 아니라 암호 연산과 관련된 기능을 지원하는 매체이다[1],[2]. 따라서 향후 WAP 프로토콜의 계층 구조가 SSL/TLS 계층을 포함하거나, 응용계층에서의 보안 기능 강화를 위해 발전하더라도 WIM은 다양한 보안 기능 지원을 보장할 수 있다.

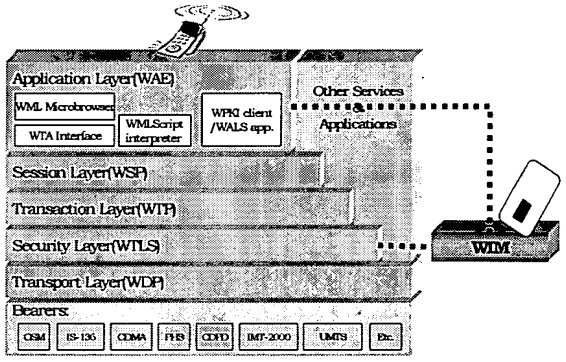


그림 1: WAP 프로토콜 참조 모델

1) WTLS 지원

WTLS 계층에서 WIM이 사용되는 시점은 핸드쉐이크 과정이다. 가입자와 서버간 핸드쉐이크는 가입자 인증과 키 설립을 위해 진행되는 과정으로써 WIM은 핸드쉐이크 과정에서의 암호연산을 수행하고 long-living WTLS 세션을 보장한다. WTLS를 지원하기 위해서 WIM이 수행하는 동작은 크게 세가지로써 첫째 비밀키의 저장 및 비밀키를 이용한 암호연산, 둘째 신뢰하는 공인 인증기관의 인증서 보관 및 인증서를 참조한 전자서명 검증, 셋째 master secret 계산과 저장 및 master secret을 이용한 주요 key material 유도 등이다.

2) 응용계층 지원

WIM은 WAP 응용계층의 요청을 받아 암호화된 데이터를 복호화하는 동작과 해쉬 데이터를 전자서명하는 동작을 수행한다. WTLS에서 제공하지 못하는 전자서명을 지원함으로써 전자상거래의 핵심 정보보호 기능인 부인방지 서비스를 보장할 수 있다. WIM은 WAP 프로토콜에서 정의하는 WMLScript를 사용한 응용뿐만 아니라 다른 모든 응용에 대한 지원을 위한 일반적인 동작을 수행한다.

2. ISO/IEC 7816

보안기능 향상을 위한 보안토큰인 WIM은 스마트카드 형태로 구현된다. 접촉형 스마트카드의 국제표준과 관련된 모든 규격은 ISO/IEC JTC1/SC17 Working Group 4에서 관리하고 있다. ISO/IEC 7816-3은 전기적 신호와 전송 프로토콜, 그리고 스마트카드와 단말기 사이에서 교환되는 정보구조를 규정하고 있다[3]. ISO/IEC 7816-4는 기본적인 산업간 명령어(Interindustry commands)를 APDU (Application Protocol Data Unit) 형태로 정의하고 있으며[4], ISO/IEC 7816-8에서는 보안기능과 관련된 산업간 명령어를 정의하고 있다[5].

접촉형 스마트카드를 구현함에 있어 ISO/IEC 7816 표준을 준용하는 것은 국제적인 호환성을 보장하기 위한 가장 중요한 부분으로써, 본 논문에서 구현하는 무선인증모듈의 소프트웨어 설계에 ISO/IEC 7816 표준을 준용하였다. 이외에도 스마트카드의 물리적 특성을 정의한 ISO/IEC 7816-1, 접점의 크기 및 위치를 정의하고 있는 ISO/IEC 7816-2, 다양한 응용의 등록 절차 및 ID 부여를 위한 규격인 ISO/IEC 7816-5가 있고, ISO/IEC 7816-6은 스마트카드와 리더 사이의 데이터 원소(Data Elements)에 관한 표준이고, ISO/IEC 7816-7에서는 SCQL (Structured Card Query Language) 데이터베이스 개념과 관련된 산업간 명령어를 정의하고 있다.

3. PKCS #15

PKCS (Public-Key Cryptography Standards) 규격은 1991년 6월에 발표되기 시작한 공개키 암호 표준의 집합으로써 RSA Laboratories가 개발, 소유 및 관리하고 있다. 특히 PKCS #15는 스마트카드와 같은 보안토큰이 저장하는 정보형식을 정의하는 공개키 암호 표준으로써 비밀키와 공인 인증기관 인증서 등을 저장하고 액세스하기 위한 방법을 정의하고 있다[6].

ISO/IEC 7816 표준은 스마트카드 구현에 있어 물리적인 특성 및 데이터 전송과 관련된 국제 호환성을 보장하는 반면, PKCS #15를 비롯한 PKCS 규격은 공개키를 사용하는 보안토큰의 정보 저장과 액세스에 대한 국제 호환성과 멀티 애플리케이션으로의 기능 확장성을 제공한다. PKCS #15에서 정의한 정보형식은 스마트카드를 비롯한 다양한 매체에 구현될 수 있으며, 스마트카드에 구현할 경우 하나의 카드에 여러 응용을 탑재할 수 있는 멀티 애플리케이션 카드 구현을 지원한다.

4. DER Encoding/Decoding

PKCS #15를 준용하는 무선인증모듈의 내부 정보형식은 ISO/IEC 7816 표준에서 정의하고 있는 DF (Dedicated Files)와 EF (Elementary Files) 개념이 적용된다. 본 논문에서 구현하는 무선인증모듈이 저장하는 중요 데이터는 EF에 저장된다. EF 내부의 데이터 구조는 ASN.1 (Abstract Syntax Notation One) 표기를 사용하여 표현할 수 있으며, 무선인증모듈에 저장되는 형태는 ASN.1 표현의 DER (Distinguished Encoding Rules) 인코딩 데이터가 저장된다[7],[8]. 따라서 무선인증모듈과 통신하는 리더는 무선인증모듈의 정보형식을 PKCS #15에 기반하여 분석하고, 분석된 결과에 따라 필요한 EF를 선택한다. EF에 저장된 DER 인코딩 데이터를 읽은 후에

DER 디코딩을 수행하여 원하는 정보를 얻게 되는데, 여기서 알 수 있듯이 DER 디코딩 동작은 리더만이 수행하므로 무선인증모듈은 DER 인코딩/디코딩 루틴을 갖고 있지 않아도 된다.

이상에서 살펴본 바와 같이 무선인증모듈을 스마트카드로 구현하기 위해서는 물리적인 특성을 비롯하여 내부 정보형식의 표현 및 저장 표준을 준수하여야 하며, 무선인증모듈이 지니는 고유의 정보보호 기능을 제공할 수 있도록 구현되어야 한다. 그림 2는 무선인증모듈을 사용하는 무선단말기와 무선인증모듈 사이의 관계를 간략하게 표현한 것이다. 본 논문에서 구현하는 PKCS #15 기반의 보안 무선인증모듈은 그림 2의 구성을 기본으로 한다.

그림 2: 무선단말기와 무선인증모듈

III. 무선인증모듈 설계

1. 설계 고려사항

무선인증모듈을 구현함에 있어 기능적인 측면에서의 고려사항은 WIM 기능을 구현하는 것이고, 구현 형태에서의 고려사항은 스마트카드 형태로 구현하는 것이다. 또한 상기 II절에서 밝힌바와 같이 호환성과 확장성을 고려하여 국제규격을 준수하여 설계한다.

그림 3은 이러한 기본적인 설계조건을 고려하여 구성한 스마트카드 명령어처리 설계도이다. 가장 먼저 고려해야 할 사항은 그 구현형태로써, 접촉형 스마트카드에 대한 전반적인 규격을 담고 있는 ISO/IEC 7816 표준을 준수하는 것이다. 그림 3에서 보이는 'WIM-ME contact point'에 해당하는 하드웨어적인 특성과 화살표로 표현하고 있는 스마트카드 명령어 전송 프로토콜, 그리고 스마트카드 내부 파일 구조 등이 ISO/IEC 7816 표준을 따르는 부분이다. 스마트카드가 보안토큰의 일반적인 형태인 만큼 내부 저장을 위한 정보형식은 PKCS #15를 준수하고, 정보형식의 저장형태는 DER 인코딩 데이터로 저장된다.

2. 설계 특징 및 장점

본 논문에서 구현하는 무선인증모듈의 설계 특징 중의 하나는 전송계층(Transport Layer)과 스마트카드 명령어처리 계층(Processing Layer)이 구분되는 계층화구조를 갖는다는 것이다. 그림 3에서 보이듯이 이러한 계층화구조 설계는 구현된 프로그램의 유지보수가 용이하며, 스마트카드 명령어처리 계층과는 독립적으로 데이터 전송률을 높이기 위하여 새로운 전송 프로토콜을 적용하기도 쉽다.

설계상의 또 하나의 특징은 WAP 포럼의 무선인터넷 보안모듈 규격인 WIM 규격과 PKCS #15 정보형식을 준수한 파일시스템과 파일 접근제어를 포함하고 있다는 것이다. 향후 PKCS #15 기반의 정보형식을 따르는 응용을 운용하는 멀티 애플리케이션 카드로의 확장성 및 호환성이 우수한 장점을 지닌다.

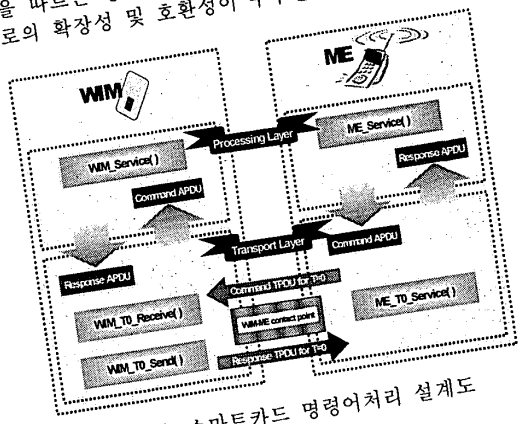


그림 3: 스마트카드 명령어처리 설계도

IV. 무선인증모듈 구현

제시된 설계에 따라 무선인증모듈을 구현하여 그 기능을 확인하기 위하여 다음과 같은 처리능력을 살펴보기로 한다. 첫째, 전송계층에서의 데이터 전송 프로토콜의 성능을 파악하는 것이고, 둘째 파일시스템에 대한 접근제어 및 정보저장 능력을 확인하는 것이며, 끝으로 정보보호 서비스 제공을 위한 정보보호 알고리즘 처리 능력을 분석하는 것이다. 본 절에서는 구현된 무선인증모듈에서의 주요 성능에 대한 분석과 그 결과를 보인다.

1. 전송계층

무선인증모듈 내부에서의 전송계층 처리는 그림 3에서 나타내고 있듯이 명령어 수신과 송신 프로토콜을 구현하는 것이다. T=0 또는 T=1 프로토콜이 사용될 수 있는데, T=0 프로토콜은 바이트 단위 전송을 기본으로 하기 때문에 요구되는 메모리의 크기가 작다는 장점이 있다. 구현된 무선인증모듈은 작은 메모리에서도 원활하게 수행되며, 대단위 데이터 전송이 요구되지 않는 WIM 기능을 고려하여 전송계층 프로토콜로써 T=0 프로토콜을 사용한다.

WIM 기능을 구현하기 위한 스마트카드 명령어는 APDU의 의미에 따라 네가지 경우로 구분할 수 있다. 전송계층에서의 T=0 프로토콜은 명령어 APDU의 길이 정보를 이용하여 네가지 경우에 따른 명령어를 구분하도록 구현되어 있다. 전송계층에서 송수신되는 데이터 유닛은 TPDU (Transport Protocol Data Unit)라 하며, 전송계층 T=0 프로토콜에서 수신된 모든 명령어 TPDU는 네가지 경우 각각에 맞게 명령어 APDU로 재구성되어 스마트카드 명령어 처리 계층으로 올려진다.

따라서 그림 3에서 보이는 WIM_Service() 함수는 전송계층에서 사용되는 프로토콜에 영향을 받지 않는다. 스마트카드 명령어처리 계층이 전송계층과 독립적으로 구현되어 있기 때문에 전송계층 프로토콜의 대체가 쉬워지는 확장 가능성이 크다는 장점이

있다.

2. 정보저장 및 접근권한

무선인증모듈에 저장되는 데이터는 사용자 인증서 정보와 같은 공개 가능한 정보뿐만 아니라 전자서명에 사용되는 비밀키 정보, 사용자 인증에 사용되는 PIN (Personal Identification Number) 정보 등과 같은 중요 정보를 포함하고 있다. 구현된 무선인증모듈은 PKCS #15 규격을 준수하여 파일구조를 유지하고 있으며, 각각의 파일에 접근하기 위한 접근권한의 현재 상태정보를 무선인증모듈 내부에서 유지하고 있다. 각각의 파일에 대한 접근제어는 정보보호 서비스 측면에서 반드시 구현되어야 하는 항목이다.

파일에 대한 접근제어란 파일 내부의 콘텐츠에 접근하여 읽기 동작 또는 쓰기 동작을 수행할 수 있는 허락 여부를 의미한다. 현재 사용자가 어떤 PIN을 입력했는가에 따라 각각의 파일에 대한 접근권한이 결정된다. PKCS #15에 따른 파일시스템 구성과 내부 정보의 DER 인코딩 저장 및 파일에 대한 접근제어는 무선인증모듈을 이용한 무선인터넷 보안기능 강화에 크게 기여할 수 있으며, 호환성이 우수하여 국제표준 규격의 무선인터넷 휴대단말기에서 보안기능 수행이 가능하다.

3. 정보보호 알고리즘

무선인터넷 보안토큰으로 사용되는 무선인증모듈을 설계하고 구현함에 있어 가장 중요하게 고려되어야 하는 기능은 국제규격의 정보보호 알고리즘을 효율적으로 구현하는 것이다. 구현된 무선인증모듈이 처리하는 정보보호 알고리즘 연산은 비대칭키 연산으로써 RSA 1024 비트 암/복호화, 전자서명/검증 처리와 key material을 계산하기 위한 PRF (Pseudo Random Function) 연산이다. RSA 1024 비트 암호화 연산과 전자서명을 위한 원천데이터는 PKCS #1 규격에서 정의한 인코딩 규칙에 따라 1024 비트로 확장된다[9]. PKCS #1 인코딩은 WIM 규격에서도 정의하고 있는 내용이며, RSA 암호화를 위한 인코딩에서는 임의의 랜덤 바이트들이 첨가되기 때문에 동일한 원천데이터라 하더라도 그 결과값은 항상 달라진다.

표 1: RSA 1024 비트 연산 결과

	Data size	Key size	Time
RSA 암호화	1024 비트	24 비트	275 msec
RSA 복호화	1024 비트	1024 비트	2.55 sec
RSA 전자서명	1024 비트	1024 비트	2.68 sec
RSA 서명검증	1024 비트	24 비트	239 msec

무선인증모듈 구현에 이용한 개발툴킷은 코프로세서를 장착한 스마트카드를 고려하고 있으며, 코프로세서는 지수승 모듈러 연산을 제공하기 때문에 RSA 연산을 하드웨어적으로 처리할 수 있다. 표 1에서 RSA 1024 비트 연산에 대한 결과를 보인다. 표 1에서 보이는 시간은 호스트 PC에서 RSA 처리 명령어를 보내고 그 결과를 받을 때까지의 시간이다. 일반적인 스마트카드 개발환경과 마찬가지로 호스트 PC와 리더는 시리얼 포트로 연결되어 있으며, 무선인증모듈 내부에서 T=0 전송계층 프로토콜을 거쳐 EEPROM에 쓰기 동작을 수행하는 과정도 있기 때문에 실질적인 RSA 연산 시간은 표 1에 보인 것보다 작을 것으로 판단된다.

V. 결론

WAP 환경뿐만 아니라 유무선 통합 환경의 인터넷 공간에서도 무선인증모듈의 사용은 필수적인 보안 요소가 될 것이다. 본 논문에서 구현한 무선인증모듈은 RSA 공개키 연산을 이용한 정보보호 서비스 제공을 기본으로 하고 있다. 그 구현 기술에 있어서 전송계층과 스마트카드 명령어처리 계층을 구분하는 계층화구조로 설계하여 T=0 프로토콜이 아닌 새로운 전송 프로토콜로의 확장이 용이하다. 특히 무선인증모듈 내부의 파일시스템은 PKCS #15 규격을 준용하고 있으며, 정보형식에 대한 DER 인코딩 데이터를 저장하기 때문에 현재의 무선인증모듈을 PKCS #15 응용을 비롯한 다양한 스마트카드 응용서비스를 지닌 멀티 애플리케이션 카드로 확장하여 정보보호 서비스와 사용자의 이동성을 충실히 보장할 수 있다.

참고문헌

[1] WAP, "Wireless Application Protocol Identity Module Specification, Part: Security, Version 02-Jan-2001," WAP Forum, Jan. 2001.

[2] WAP, "Wireless Application Protocol Wireless Transport Layer Security Specification, Draft Version 02-Jan-2001," WAP Forum, Jan. 2001.

[3] ISO/IEC 7816-3, "Information Technology - Identification cards - Integrated Circuit(s) cards with contacts - Part 4: Interindustry commands for interchange, International Organization for Standardization," Dec. 1995.

[4] ISO/IEC 7816-4, "Information Technology - Identification cards - Integrated Circuit(s) cards with contacts - Part 3: Electronic signals and transmission protocols, International Organization for Standardization," Sep. 1995.

[5] ISO/IEC 7816-8, "Identification cards - Integrated Circuit(s) cards with contacts - Part 8: Security related interindustry commands, International Organization for Standardization," Oct. 1999.

[6] RSA Laboratories, "PKCS #15 v1.1: Cryptographic Token Information Syntax Standard," Jun. 2000.

[7] ISO/IEC 8825-1, "Information Technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)," Dec. 1998.

[8] ISO/IEC 8824-1, "Information Technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation," Dec. 1998.

[9] RSA Laboratories, "PKCS #1 v2.0: RSA Cryptography Standard," Oct. 1998.